Cybersecurity and skills gap in Europe: Facts & figures

Gianluca Dini
University of Pisa, Italy

Relevant Facts&figures

Skill Gap is 142k just in EMEA

The gap (2018) of cybersecurity Professionals is estimated 142k just in EMEA…

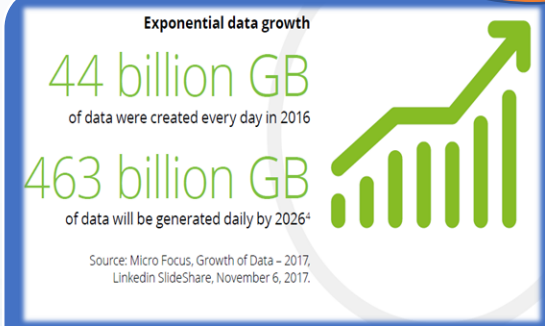
and is expected to grow in 2019

Source: (ISC)² Cybersecurity workforce study, 2018

$ 600 Billion

Source: McAfee and the center for Strategic and International Studies, 2018

463 Billion Gb of data by 2026



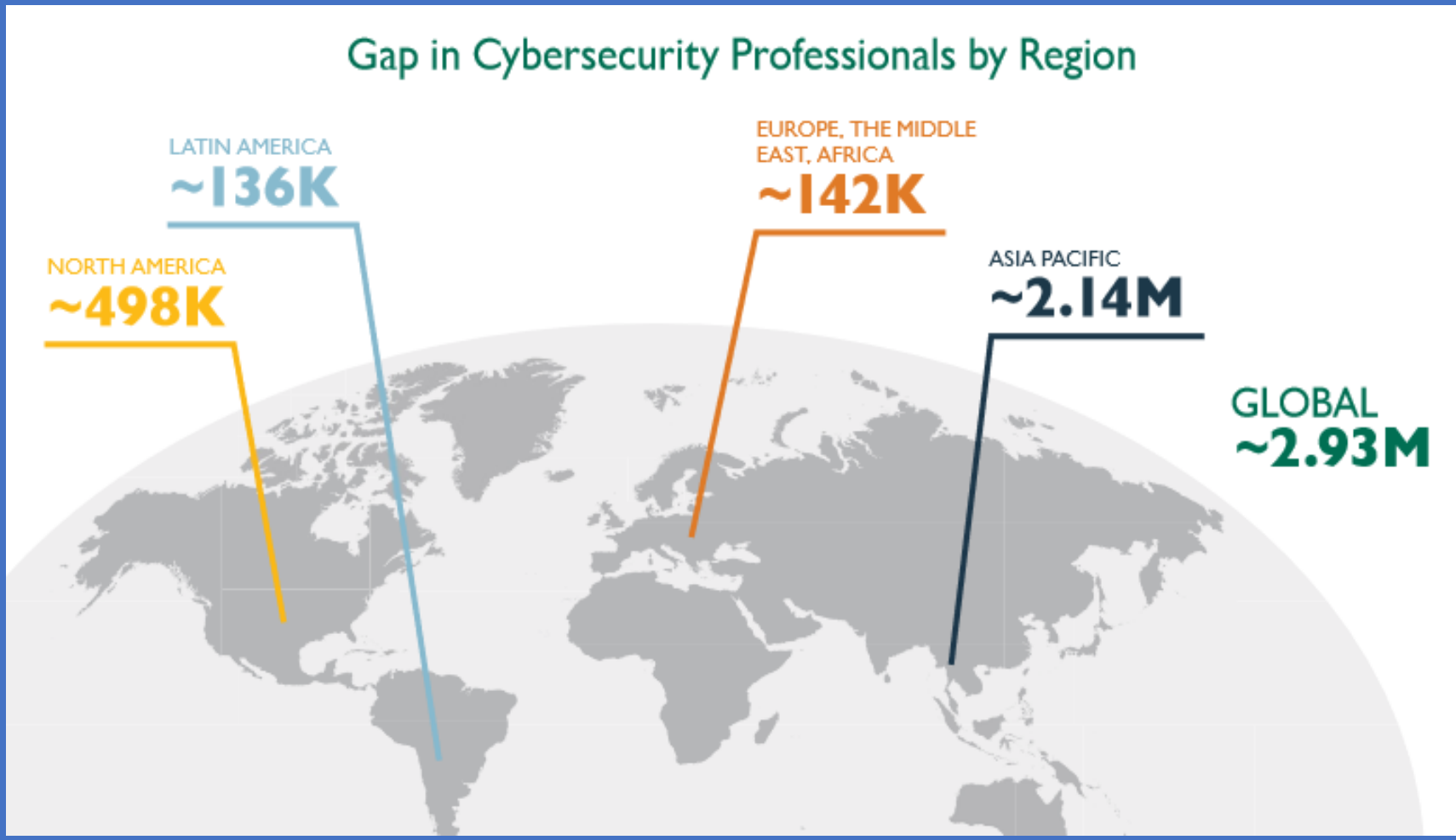
Source: Micro Focus, Growth of data – 2017, Linkedin SlideShare, November 6, 2017

Skill Gaps ask for new cybe training programmes

The SA Computer Based Training market is estimated to grow 47% in 2019 ($660 million)

Source: Gartner Security Awareness CBT report

Gap in Cybersec Professionals, by Region



Source: (ISC)² Cybersecurity workforce study, 2018

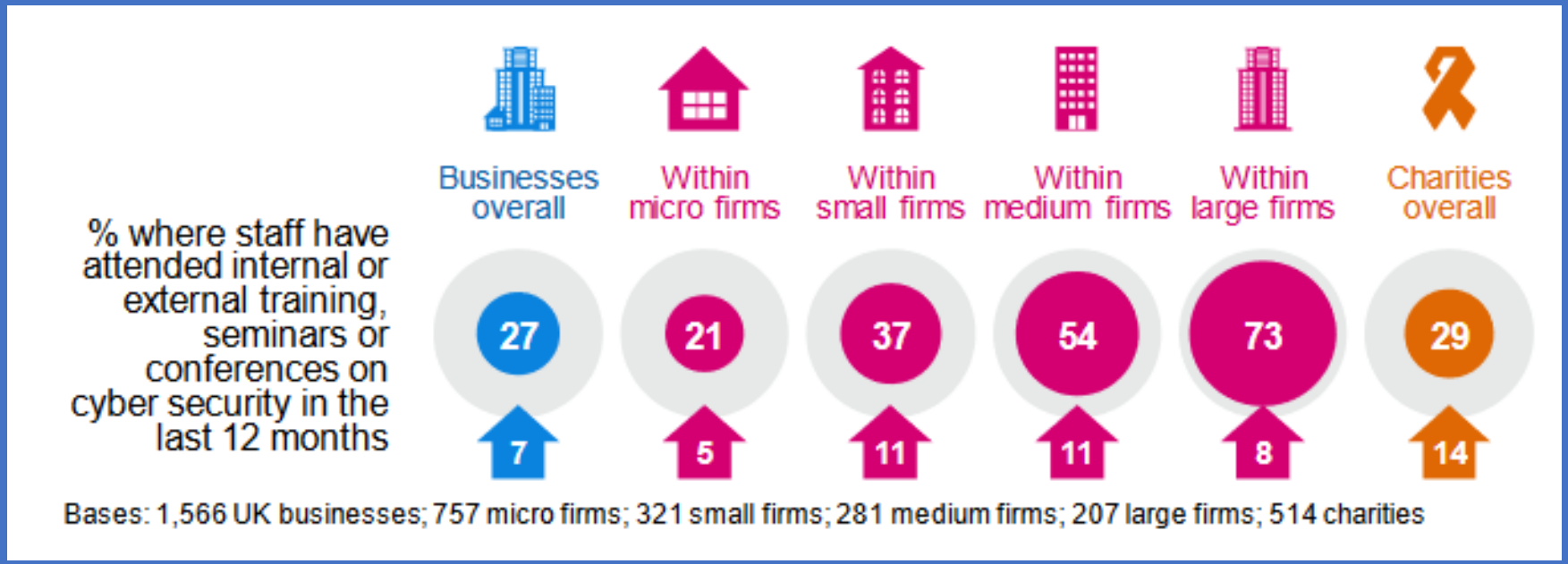
Customisation is the way!

Jeweler's perspective on theft security	Corporate perspective on cyber security
I know which assets to protect and have set up the appropriate measures.	I take measures without a having a clear idea of the assets it is essential to protect.
I perceive theft as a risk in the business and know that realistically I can't be in business if I want 100 percent security.	I see cyber crime as something exotic and strive to achieve 100 percent security.
I focus on measures that prevent a person from leaving with valuable goods.	I focus on measures that prevent a person from entering and forget to take measures that prevent a person from taking away information.
I do not let security suppliers spook me and I make my own purchasing decisions.	My security policy depends on the tools available in the marketplace, without knowing exactly what I need.
When it goes wrong or almost goes wrong, I learn a lesson.	When it goes wrong or almost goes wrong, I panic.
I train employees in how to reduce the risk of theft and talk to them when they make mistakes.	I view cyber security as mainly a matter for specialist professionals and don't want to burden the rest of the organization with it.
I invest in tools because they assist the continuity of my business.	I invest in tools because it is mandatory and because the media reports on incidents every day.

Source: KPMG Cyber security: it's not just about technology

Company size and cybersecurity training

Organisations where staff have had cyber security training in the last 12 months



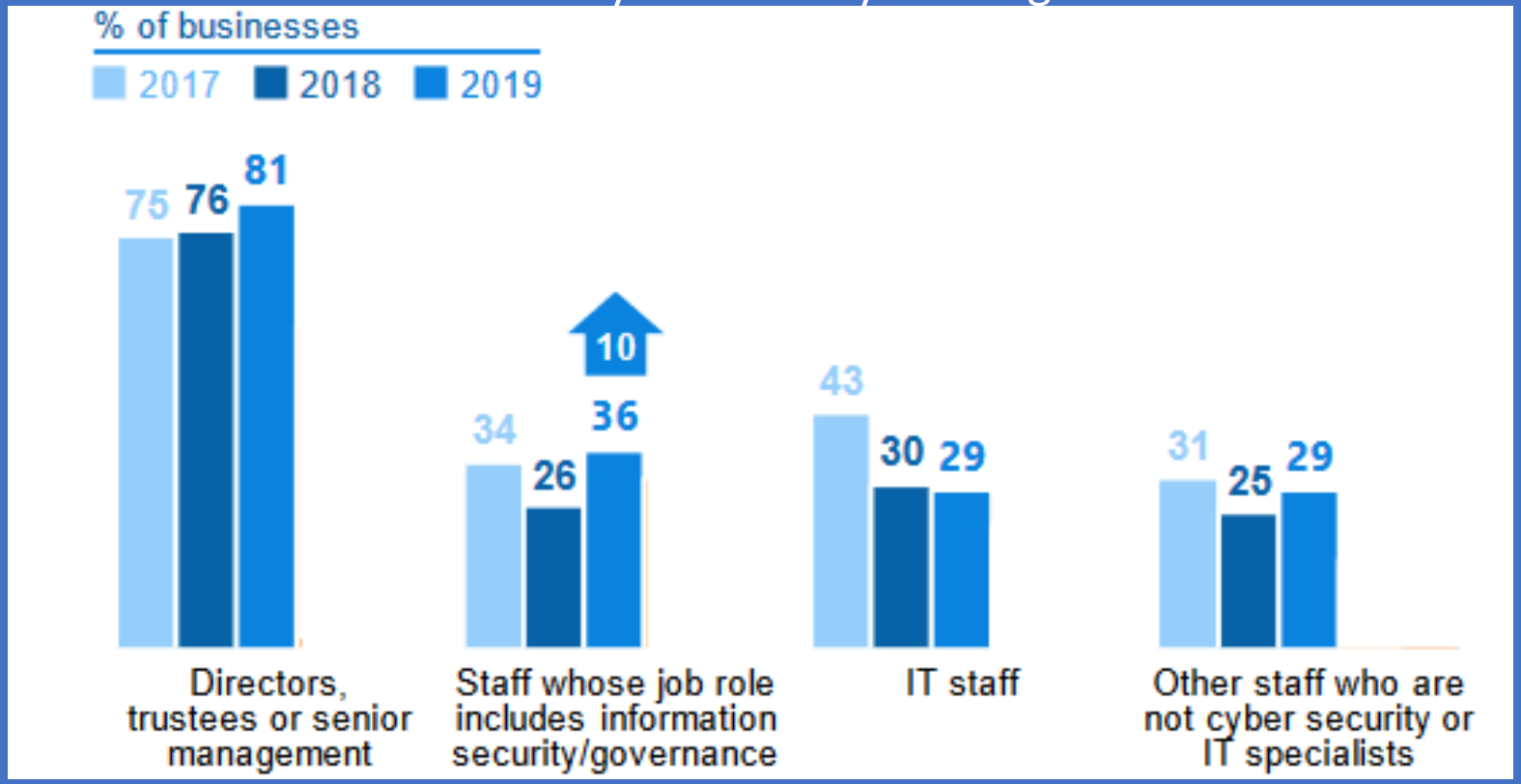
Source: Cyber Security Breaches Survey 2019 – Department for Digital, Culture, Media & Sport

Large Enterprises have more resources to dedicate to Cyber Security Training than SMEs.

CYBERWISER.eu aims at removing this barrier, lowering costs and accessing to innovative solutions for Cyber Security Training

Cyber security training – Who is trained?

Which Individuals receive cyber security training where it is offered

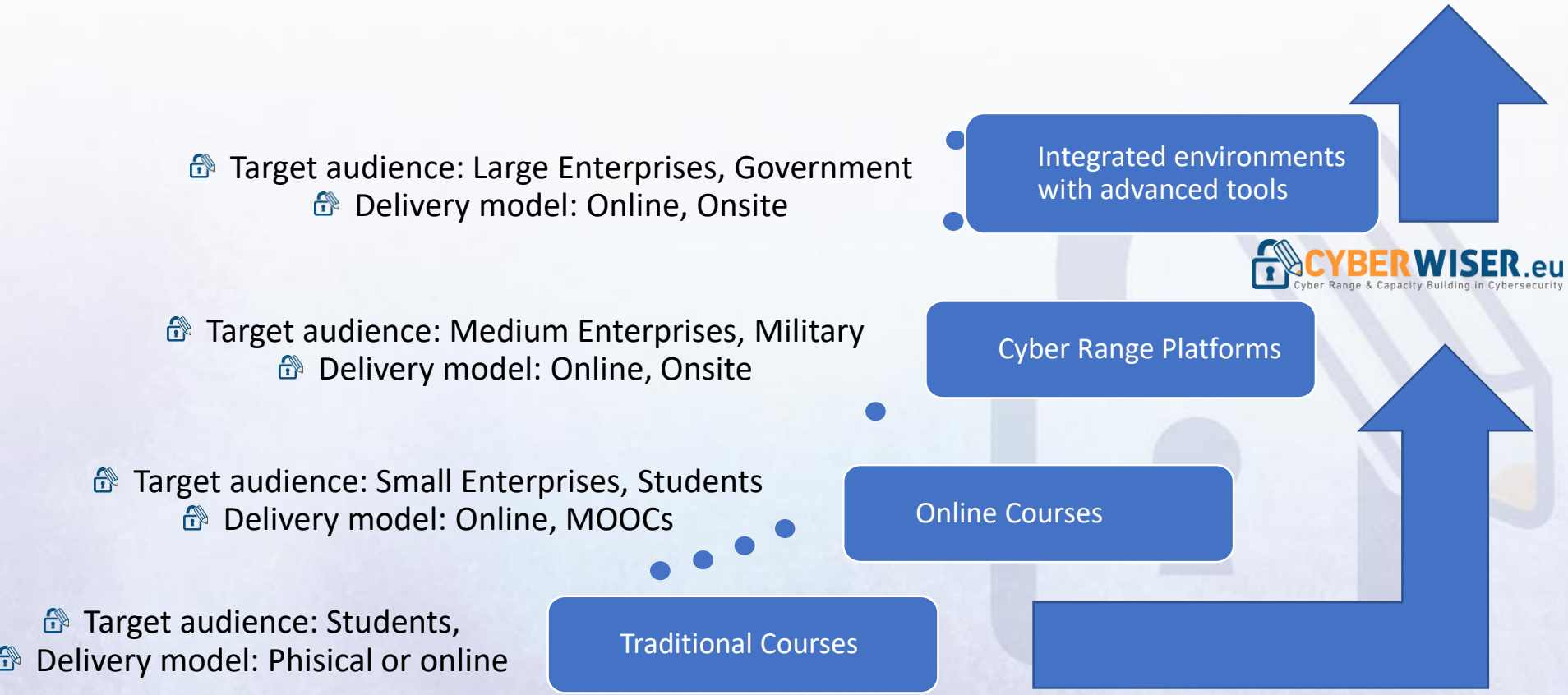


Source: Cyber Security Breaches Survey 2019 – Department for Digital, Culture, Media & Sport

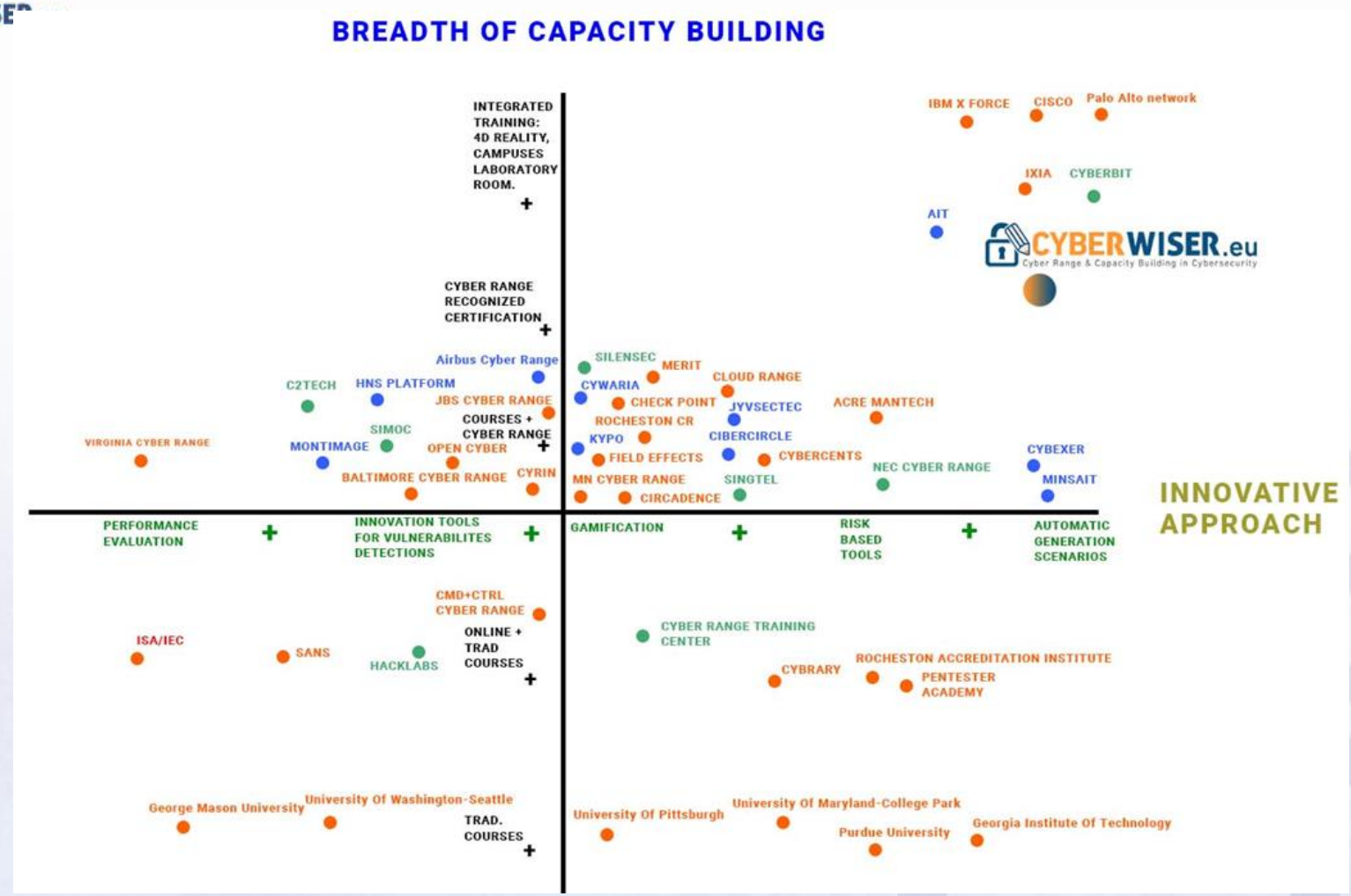
Cyber training appears to be addressed mainly to Directors and Senior management

Increasingly sopisticated solutions

High level innovation potential:
Focus on private business and individual learners
Fully integrated nature of the product offering



Positioning Analysis



Orange = North American Platform
Green = Rest of the World Platform
Blu = European Platform

Innovative approach including risk-based tools and automatic generation of scenarios is the new frontier of training