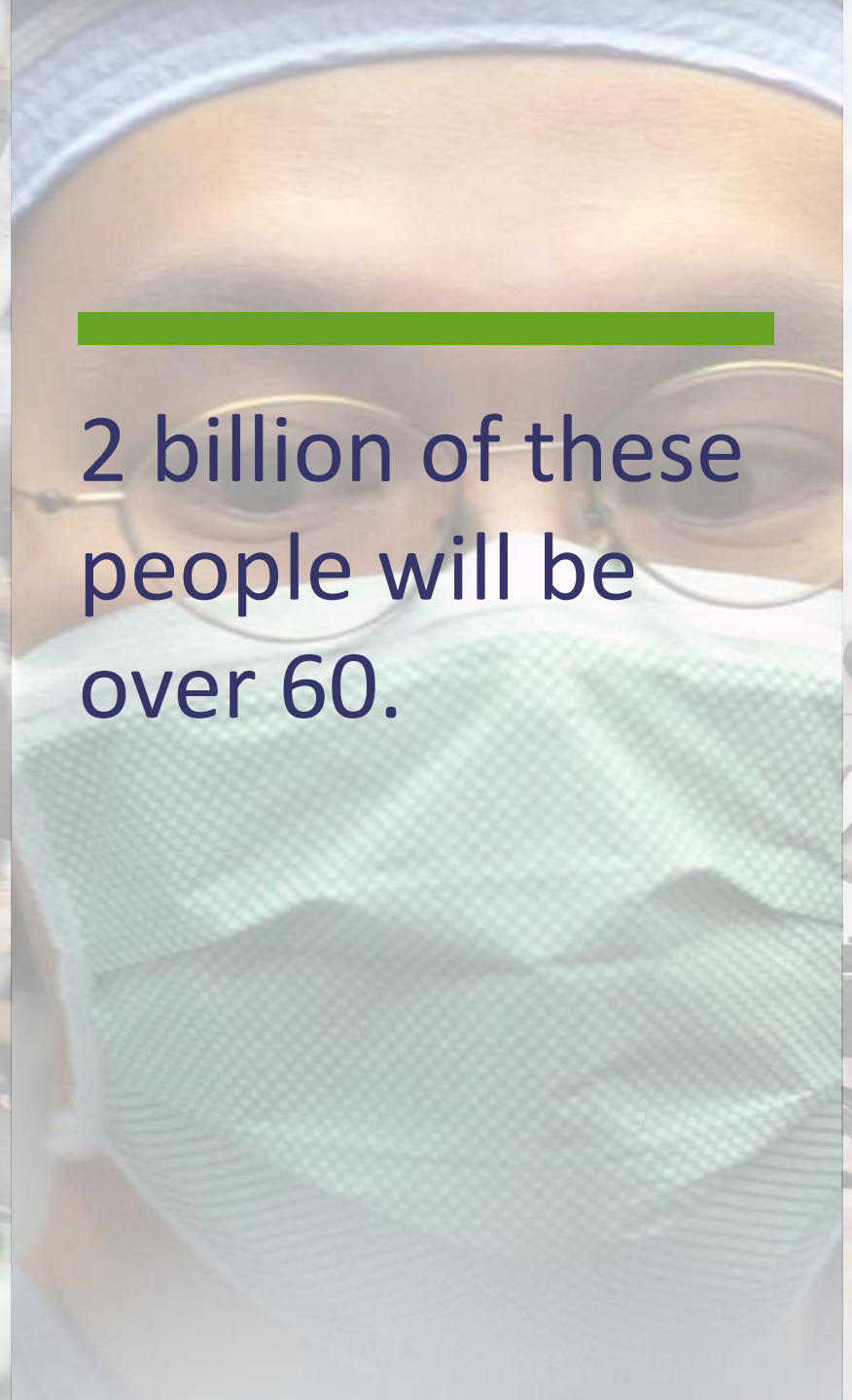
Industry 4.0 – What's next?

MYSYNERGY
Consulting in health & care

The global population will grow to more than 9 billion people by 2050.



2 billion of these people will be over 60.

73% of all deaths will be caused by chronic disease by 2020.

Source: World Health Organization

The reality of todays existing mHealth point solutions:

21% of people surveyed in the US have purchased a health-wearable, with 52% of those persons neglecting to use it on a daily basis. Tucked into this 52% of persons are 10% who have stopped using their device altogether.

Source: The wearable future, pwc research notes; survey included over 1,000 consumers in the US

Acquire, Analyze and Act – The Value is in the Data

Acquire

Effectively, rapidly and efficiently acquire and consolidate massive amounts of patient related data

Analyze

Achieve real results to get the insights you need with a variety of means alone or in combination

Act

Real-time response time regardless of data volume or data location manage and integrate massive volumes of data

Digital technology can bridge the gap of time and distance between clinicians and consumers

1. Put diagnostic testing of conditions into the hands of patients

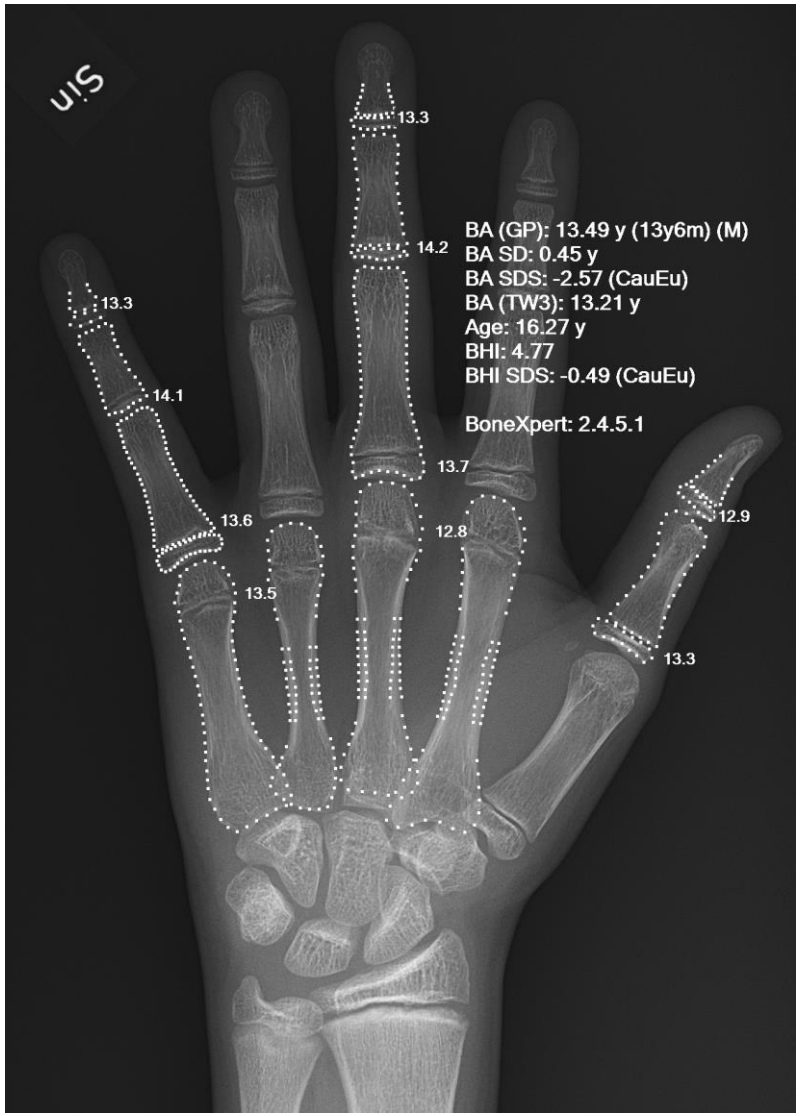
2. Increase patient-clinician interaction

3. Promote self-management of chronic disease using health apps

4. Help caregivers work more as a team

5. Generate actionable insights through analytics to yield better outcomes

X-ray of a hand, with automatic calculation of bone age by a computer software.



https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare#/media/File:X-ray_of_a_hand_with_automatic_bone_age_calculation.jpg

What is #AI?

#AI is the ability for computer algorithms to approximate conclusions without direct human input.

#AI uses #ML algorithms to gain and process information

#AI algorithms need to be tested repeatedly

algorithms are literal – they can't adjust itself

algorithms are black boxes – they can predict extremely precise, but not the cause or the why

If Software “is eating” or “programs” the world, are we safe ?

2011

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

ESSAY

Why Software Is Eating The World

By MARC ANDREESSEN

August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.

In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc

In short, software is eating the world.

More than 10 years after the peak of the 1990s dot-com bubble, a dozen or so new Internet companies like Facebook and Twitter are sparking controversy in Silicon Valley, due to their rapidly growing private market valuations, and even the occasional successful

2016

ANDREESSEN HOROWITZ

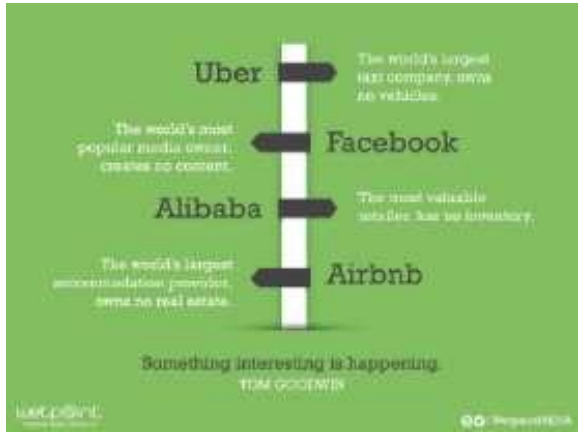
Software Is Eating the World

MACHINE & DEEP LEARNING

a16z Podcast: Software Programs the World

with Marc Andreessen, Ben Horowitz, Scott Kupor, and Sonal Chokshi

"All of a sudden you can program the world" — it's the continuation of the software eating the world thesis we put out over five years ago, and of the trajectory of past and current technology shifts. So what are those shifts? What tech trends and platforms do we find most interesting on the heels of raising our fifth fund? Are we just building on and extending existing platforms though, or will there be new platforms; and if so, what will they be? Well, distributed systems for one...




A SHIP IS
SAFE
IN HARBOR BUT ...
THAT'S NOT WHAT
SHIPS
ARE BUILT FOR.
- John A. Shedd
Photo © the_tahoe_guy (Flickr)
vagabondish

Triton > Trisis (the malware, "designed to kill")

https://www.cisoplatform.com/profiles/blogs/triton-how-it-disrupted-safety-systems-and-changed-the-threat-lan

the cyberwire

TRISIS/TRITON and the rise of malware built to kill.

November 1, 2018.

By The CyberWire Staff

What lessons does the TRISIS/TRITON attack on a Middle Eastern petrochemical facility hold for industry? Speakers at SecurityWeek's ICS Security Conference think there are at least three. First, hunt behaviors, not signatures. Second, the barriers to effective attacks on safety instrumentation systems have dropped. And third, there's now malware out there that's been built to kill.

Hunting for Xenotime.

In November 2017 a team from industrial cybersecurity firm Dragos discovered highly tailored malware deployed against a petrochemical facility in the Middle East. They called the malware "TRISIS" because the system it affected was Schneider Electric's Triconex safety instrumented system. The malware

https://thecyberwire.com/events/ics-security-2018/trisis-triton-and-the-rise-of-malware-built-to-kill.html

ICS CYBER SECURITY CONFERENCE

About Agenda Events Hotel & Venue Contact Register

UNCATEGORIZED

Hackers Behind Triton ICS Malware Hit Additional Critical Infrastructure Facility

April 10, 2019 / 0

Triton Hackers Focus on Maintaining Access to Compromised Systems, Report Says

(SecurityWeek – Eduard Kovacs) – The tools and techniques used by the threat group behind the notorious Triton malware show that the hackers are focused on maintaining access to compromised systems, according to FireEye.

The existence of Triton, also known as Trisis and HatMan, came to light in 2017 after the malware had caused disruptions at an oil and gas plant in Saudi Arabia. FireEye's Mandiant was called in to investigate the incident and the company has been tracking the threat ever since.

FireEye revealed on Wednesday that it recently responded to another attack carried out by the Triton group against a critical infrastructure facility.

The cybersecurity firm says it has come across several custom tools used by the threat actor, including ones designed for credential harvesting (SecHack, WebShell), remote command execution (NetExec), and several backdoors based on OpenSSH, Bitvise, PLINK and Cryptcat. The attackers have also relied on widely available tools, such as Mimikatz.

https://www.icscybersecurityconference.com/hackers-behind-triton-ics-malware-hit-additional-critical-infrastructure-facility/

AI makes it more complicated: in sectors

BRIEFING

European Parliament

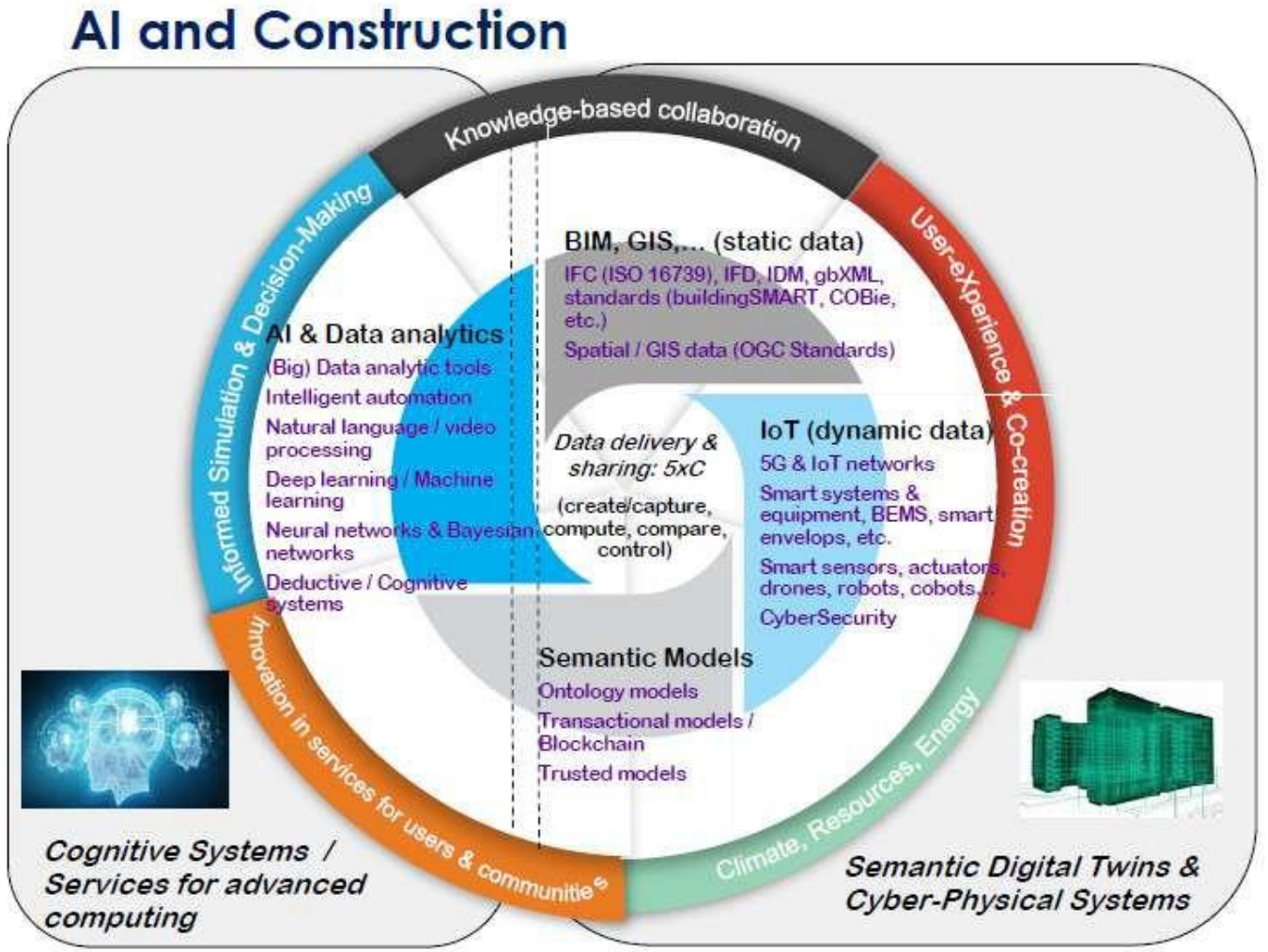
Artificial intelligence in transport

Current and future developments, opportunities and challenges

SUMMARY

Artificial intelligence is changing the transport sector. From helping cars, trains, ships and aeroplanes to function autonomously, to making traffic flows smoother, it is already applied in numerous transport fields. Beyond making our lives easier, it can help to make all transport modes safer, cleaner, smarter and more efficient. Artificial intelligence-led autonomous transport could for instance help to reduce the human errors that are involved in many traffic accidents. However, with these opportunities come real challenges, including unintended consequences and misuse such as cyber-attacks and biased decisions about transport. There are also ramifications for employment, and ethical questions regarding liability for the decisions taken by artificial intelligence in the place of humans.

The EU is taking steps to adapt its regulatory framework to these developments, so that it supports innovation while at the same time ensuring respect for fundamental values and rights. The measures already taken include general strategies on artificial intelligence and rules that support the technologies enabling the application of artificial intelligence in transport. In addition, the EU provides financial support, in particular for research.



www.ectp.org/fileadmin/user_upload/documents/ECTP/Miscellaneous_doc/ECTP-EeB_AI-in-Industrial_Technologies_FINAL.pdf

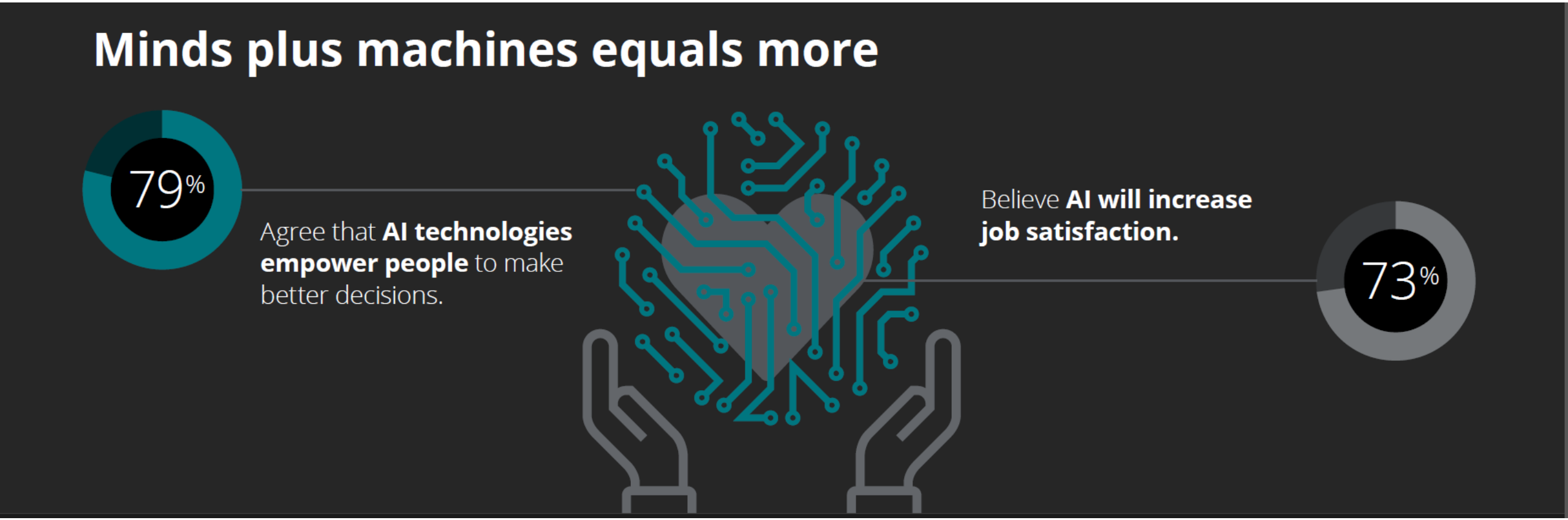
Positive return on AI investments

Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

Cybersecurity tops AI concerns

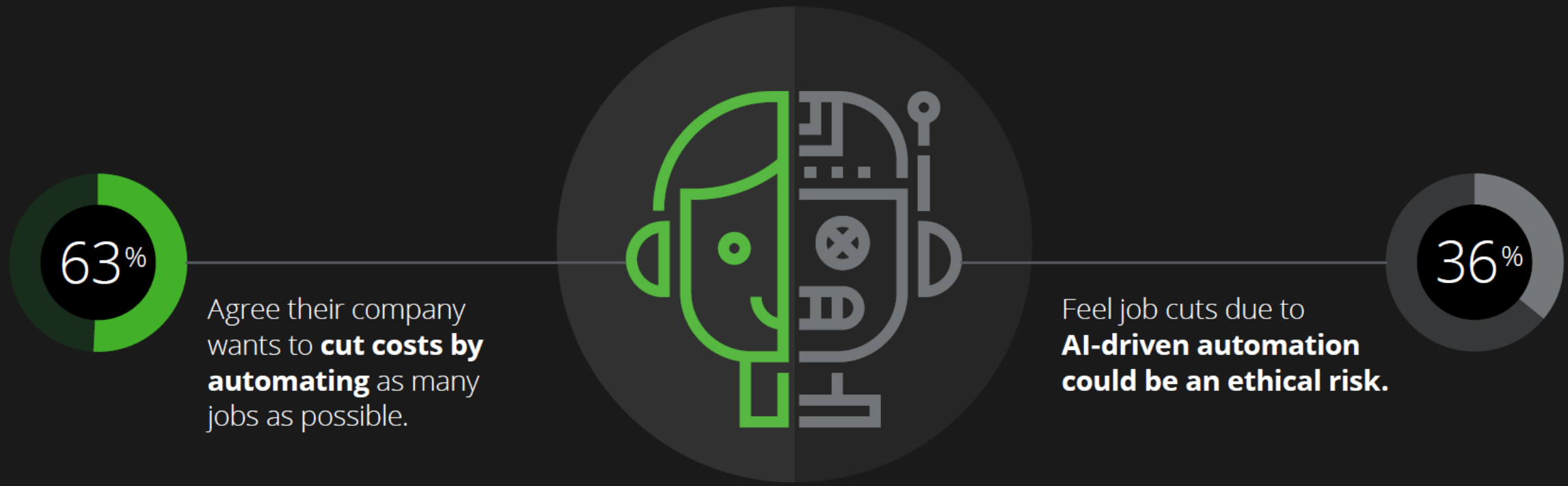
Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

Minds plus machines equals more



Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

The automation dilemma



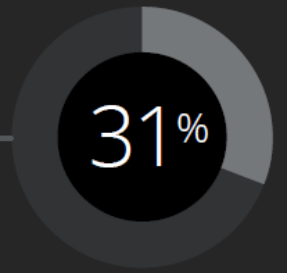
Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

Talent: more help wanted

4 in 10

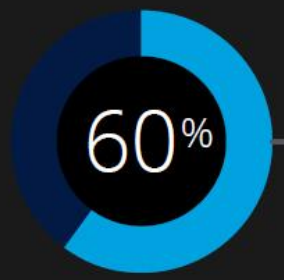
Have a high level of **confidence in their people's ability** to select, build, and manage AI solutions.

View lack of AI skills as a **top-three concern.**

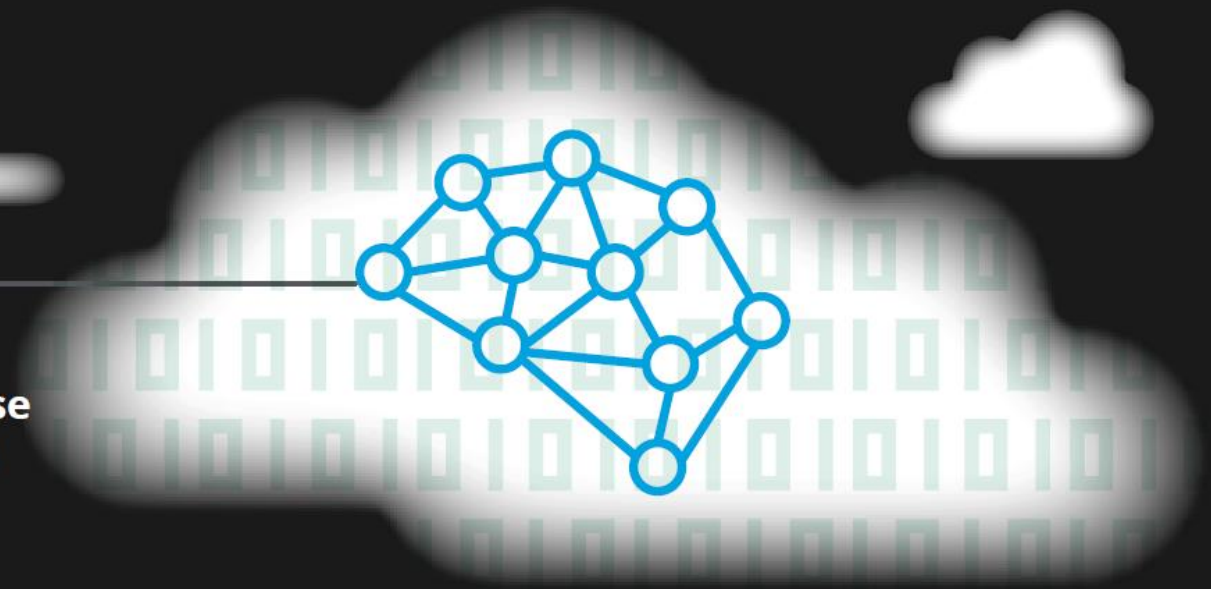


Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

Cloud jumpstarts AI adoption



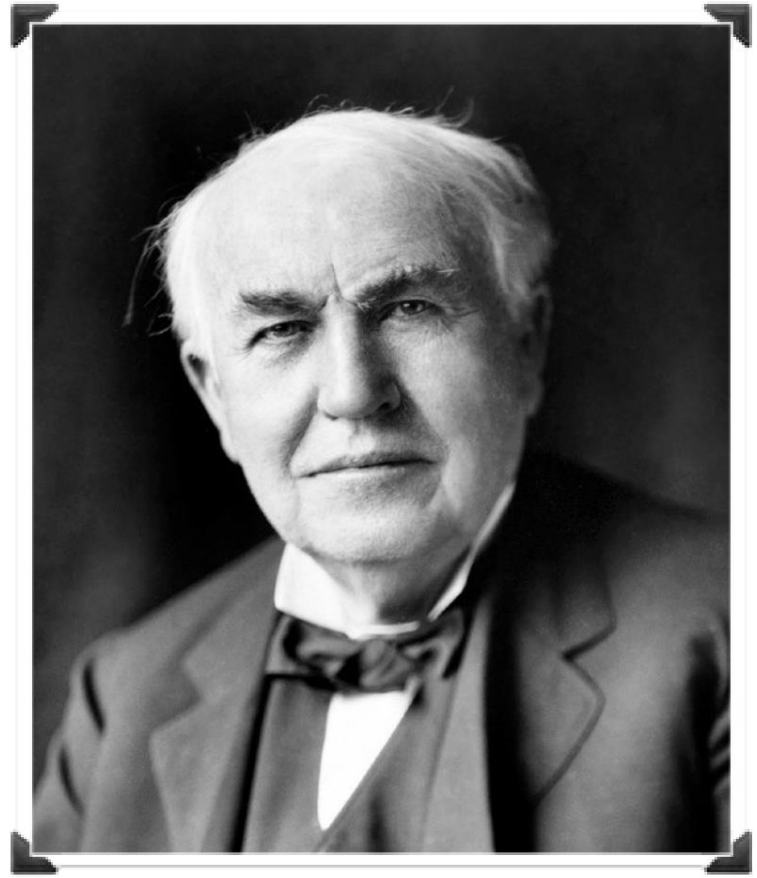
Are **getting a foothold through cloud-based, AI-enhanced enterprise software** that requires a lower upfront investment and less expertise.



Deloitte Insights State of AI in the enterprise. Deloitte, 2018.

Insights from images and sounds unleashed

Deloitte Insights State of AI in the enterprise. Deloitte, 2018.



Thomas Edison, 1847-1931

‘A vision without execution is a hallucination’

Thank you

MYSYNERGY

Yordan Iliev

Digital Health Evangelist | Strategist | Speaker | Mentor | Co-founder & CEO

Yordan.iliev (at) MYSynergy.bg