DETECT TECHNOLOGIES

Reimagining global industrial productivity

AI – An Inevitable future for Cybersecurity

Exponential trends in global AI Cybersecurity

US National Defence Strategy says "**AI will ensure that USA is able to fight and win the wars of future**"

5.08 Bn
Is estimated AI security market in 2020. Is expected to be 14.18 Bn in 2026

10.52 Mn
Large Security Malware attacks globally in 2018

$6 Trillion
Cybercrime Losses in 2021 to global GDP

Opportunity in APAC:

- CISCO reports 6 threats every minute in APAC
- 51% of all cyber attacks result in $1mn+ losses
- Growing Digital Transformation along with ineffective cyber laws and lacks of cyber security awareness makes APAC 80% more likely to be vulnerable to cybersecurity attacks

What is AI

AI is a very popular, often misused buzzword at the moment

1. AI Systems are iterative and Dynamic:

They get smarter with the more data they analyze, they “learn” from experience, and they become increasingly capable and autonomous as they go.

2. Data analytics (DA), on the other hand:

is a static process that examines large data sets in order to draw conclusions about the information they contain with the aid of specialized systems and software. DA is neither iterative nor self-learning.

Forms of AI

1. **Assisted intelligence**, widely available today, improves what people and organizations are already doing.

2. **Augmented intelligence**, emerging today, enables people and organizations to do things they couldn't otherwise do.

3. **Autonomous intelligence**, being developed for the future, features machines that act on their own. An example of this will be self-driving vehicles, when they come into widespread use.

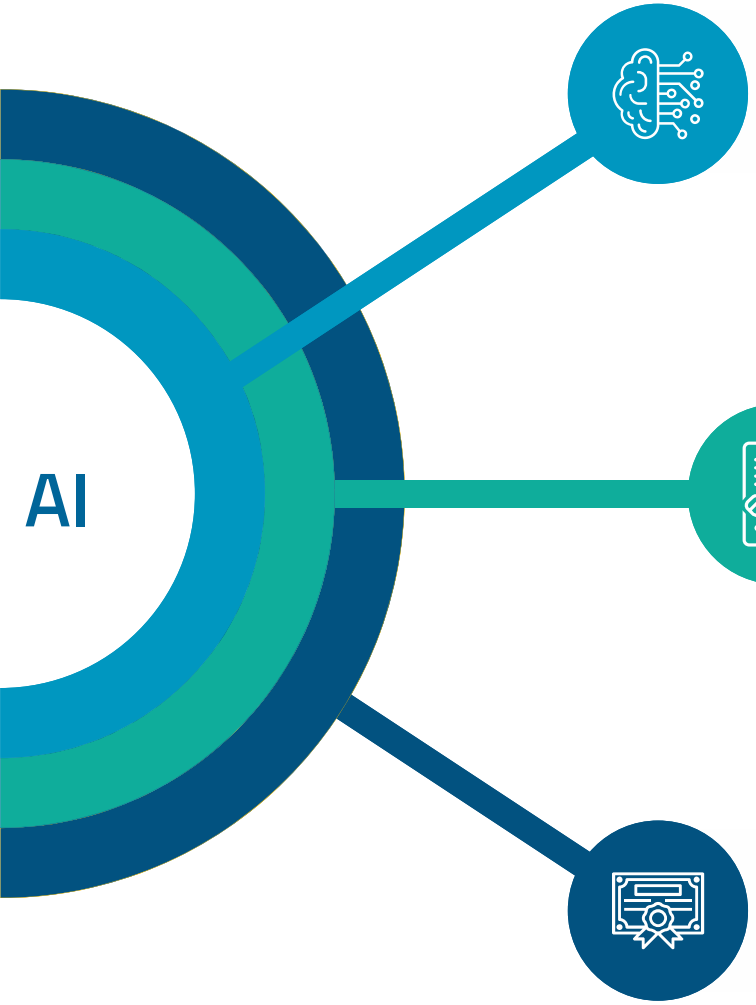
4. **Machine learning** uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance) using data rather than being explicitly programmed. Machine learning works best when aimed at a specific task rather than a wide-ranging mission.

5. **Expert systems** are programs designed to solve problems within specialized domains. By mimicking the thinking of human experts, they solve problems and make decisions using fuzzy rules-based reasoning through carefully curated bodies of knowledge.

6. **Neural networks** use a biologically-inspired programming paradigm which enables a computer to learn from observational data. In a neural network, each node assigns a weight to its input representing how correct or incorrect it is relative to the operation being performed. The final output is then determined by the sum of such weights.

7. **Deep learning** is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Today, image recognition via deep learning is often better than humans, with a variety of applications such as autonomous vehicles, scan analyses, and medical diagnoses.

Applications of AI in Cybersecurity



Authentication, Password Protection and Network Security

Vulnerability management & Phishing Detection and Control

Behavioral Analytics

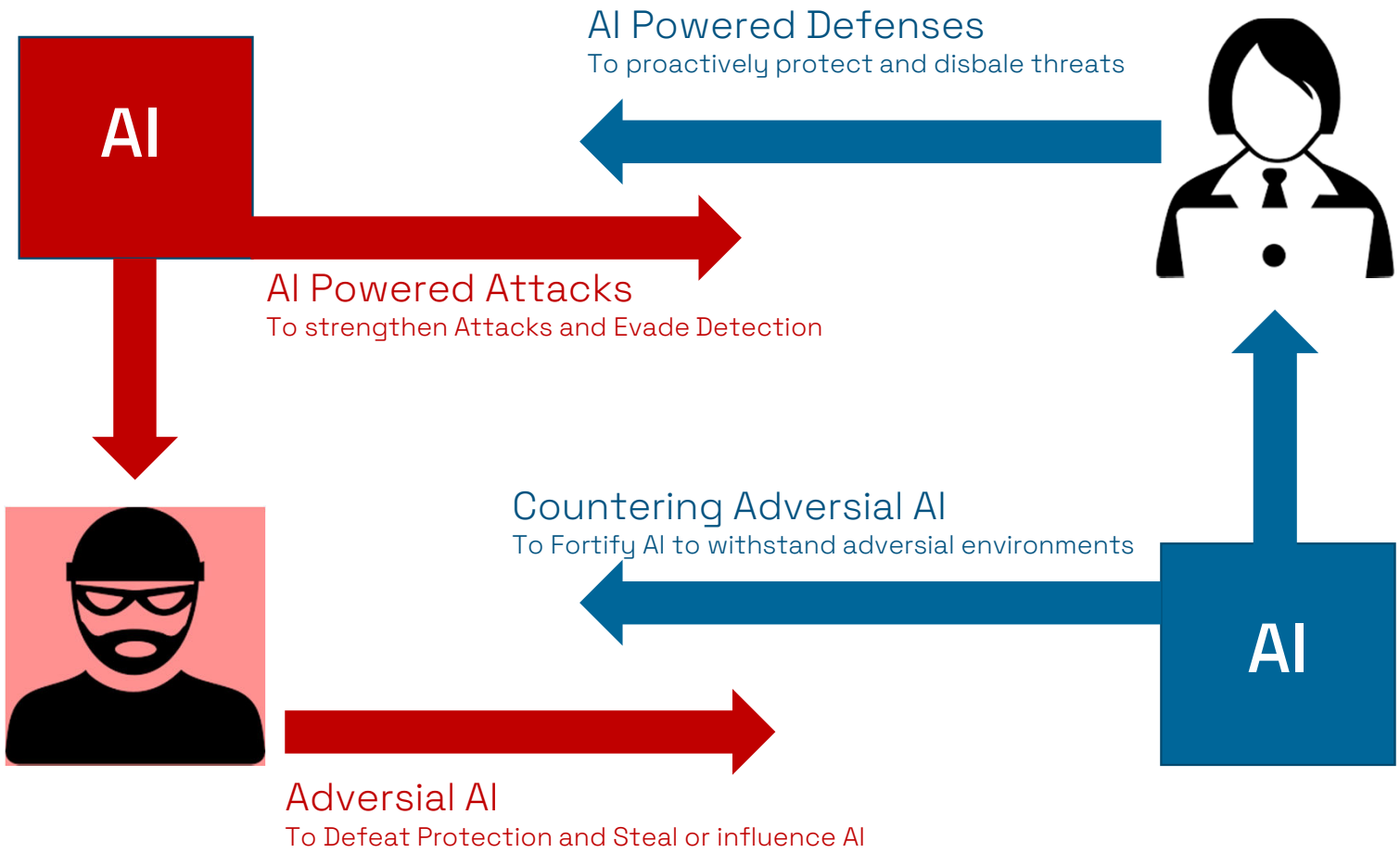
Advantages of AI in Cybersecurity

Handling multi dimensional and multi variety data with no human intervention

Targeted application with autonomous continuous improvement

Easily identifies trends and patterns and correlates to behavioral analytics

Countering Threats



Battling Bots

World has already witnessed:

1. Nachi Worm: RPC Vulnerability, Blaster Removal and Installed Patches

2. Mirai: a zombie malware strain that enslaved Internet of Things (IoT)

3. Reaper and IoTroop : Computer worms built to spread automatically, still to be unleashed completely

Bots are becoming the fastest growing trends with intelligent reasoning, messaging and conversational interfaces

Breach Risk Prediction

Cameras

Mobile

Drones

Social Media

Mails and Connected Networks

Sensors/Routers

Data Flow

ML Data Lake

- **Threat Detection** as per defined parameters
- **Loophole Detection**
- **Abnormality and Vulnerability**
- **Potential Presence of Hackers in the system**

International Benchmarking for Vulnerability Detection

Secure IT infrastructure

Governement Cloud Systems

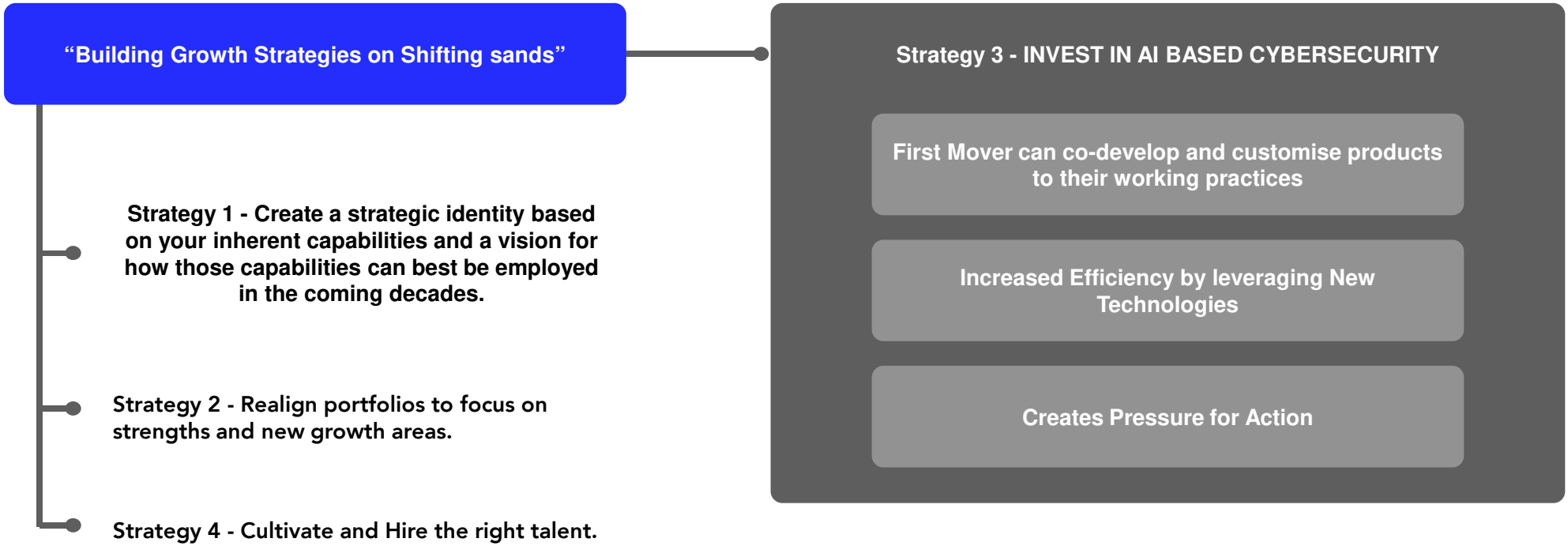
Downsides of AI in Cybersecurity

1. **Cybercriminals are AI-savvy too**: AI Solutions for security can be used by hackers, too. The practices of cybersecurity teams are a lot more open than those of cybercriminals. We are unlikely to benefit from hackers' experience, whereas they could potentially tap into organizations' progress and reverse their findings to create a better threat.

2. **Cyberthreats evolve**: even if you introduce AI to your business, it doesn't mean you automatically become immune to all threats. Viruses and malware improves all the time, and even AI systems will need constant redesign, improvement, and maintenance.

3. **High adoption barrier**: Aritifcual Intellignece still requires al lot of human resources and computing power, compared to typical antiviruses. You can simply install a ready software rather than spend time and money on building a custom AI solution. The good news, however, is that AI becoming increasingly more available and even small businesses can afford to build a security neural network.

How to Win

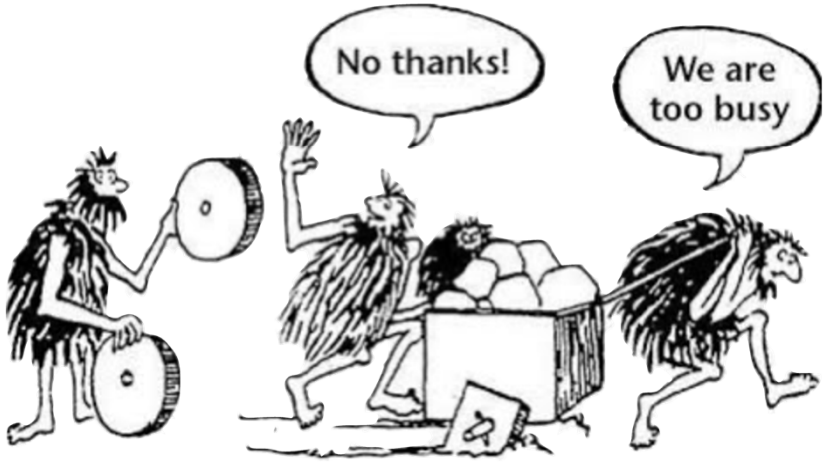

"Building Growth Strategies on Shifting sands"
Strategy 1 - Create a strategic identity based on your inherent capabilities and a vision for how those capabilities can best be employed in the coming decades.
Strategy 2 - Realign portfolios to focus on strengths and new growth areas.
Strategy 4 - Cultivate and Hire the right talent.
Strategy 3 - INVEST IN AI BASED CYBERSECURITY
First Mover can co-develop and customise products to their working practices
Increased Efficiency by leveraging New Technologies
Creates Pressure for Action

How to Win

STRATEGISE → **IMPLEMENT** → **ENSURE QUALITY**

- Problem Analysis
- Technology Analysis
- New Technology Adoption
- Technology Validation
- Technology scaling and co-development

"The greatest growing engine of change - Technology - is a powerful tool with which one can change the world. The power to use any tool, however, rests ultimately with the human hand."



Thank you!