AI for cybersecurity
Keys to success

Samuel Marchal
Research Team Leader @VTT

AI in cybersecurity: a long history

Spam/phishing

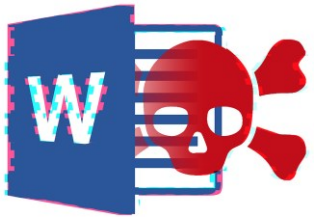
(N)IDS

Endpoint anomaly

2000

Malware

Websites/DNS



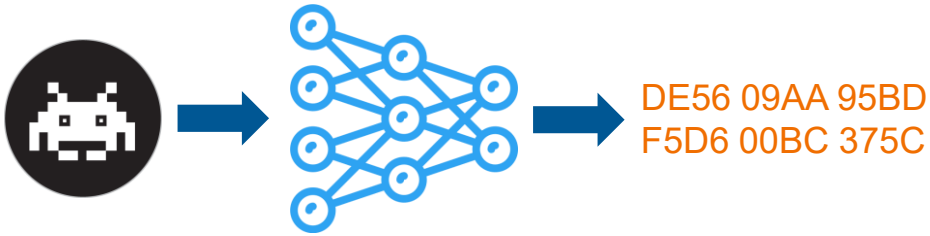
Documents

Expected benefits from AI in cybersecurity

- Speed and Automation
- Scale and Complexity
- Adaptability
- Efficient resource utilization
- Discovery of new attacks/threats

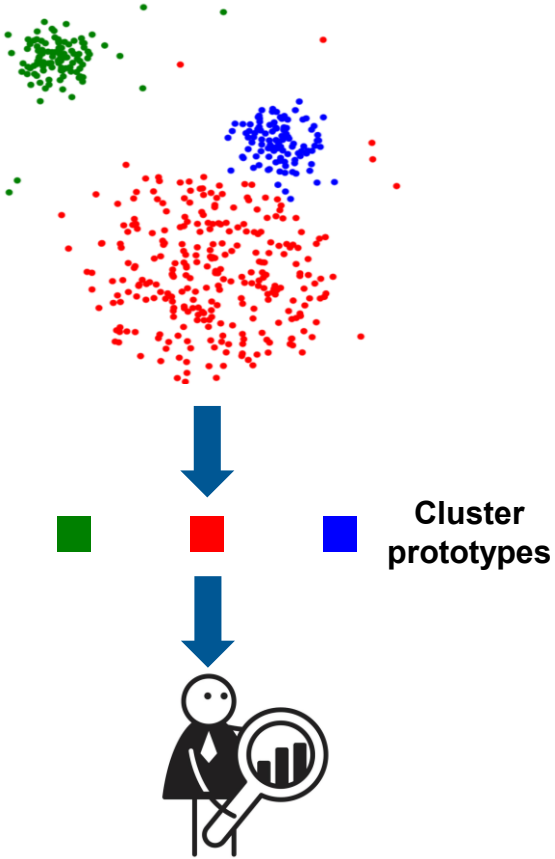
Successful applications

Malware signature extraction (pattern recognition)



Security alert reduction (statistical distribution)

Security event aggregation (clustering)



Blockers to widespread AI adoption

Unrealistic expectations

Accuracy of decisions

Inflated abilities

Autonomous adaptability

Underestimated challenges

Data acquisition & quality

Integration with technology and experts

Maintenance

Lack of understanding

AI capabilities

ML reasoning

Suitability to security problems

Keys for success: Planning

Problem understanding

Consider application criticality

AI performance linked to business objectives

Requirements for deployability

Keys for success: Development

Ensure relevance, availability, and quality of data

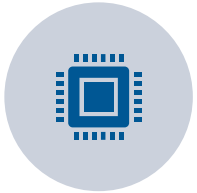
Know your data and its evolution

Avoid complexity

Deploy early

Keys for success: Operation

Be flexible with deployment and response options

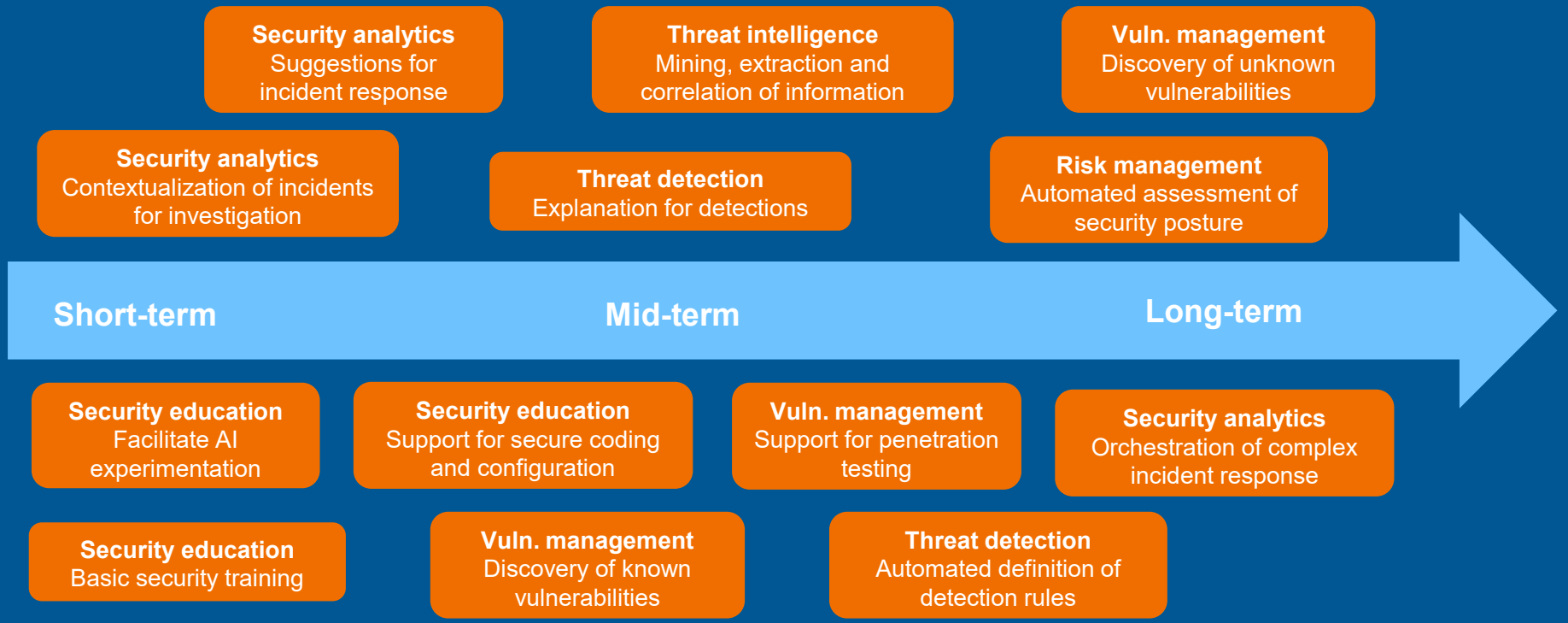


Be mindful of processing and computation costs

Develop dual skills

Develop tools and processes for recurrent tasks

LLMs: A new opportunity



Takeaways

- Reaping AI benefits in cybersecurity is possible… but challenging
  - Don’t give in to the hype
  - Data is not enough
  - Focus on your problems and business objectives
  - Develop dual skills + build expertise & experience
- Competitive advantage might be difficult to obtain now… but new AI technologies, e.g., LLMs gives new opportunity
- Comprehensive report coming up in April!

TRAFICOM
Finnish Transport and Communications Agency

Applying Artificial Intelligence in Cybersecurity