# Al for cybersecurity Keys to success

Samuel Marchal Research Team Leader @VTT

03/04/2024 VTT – beyond the obvious



### Al in cybersecurity: a long history

#### Spam/phishing



### (N)IDS



#### **Endpoint anomaly**



#### 2000



Malware



Websites/DNS



**Documents** 



## **Expected benefits from AI in cybersecurity**



Scale and Complexity

Adaptability

Efficient resource utilization

Discovery of new attacks/threats



### **Successful applications**

Malware signature extraction (pattern recognition)



Security alert reduction (statistical distribution)







### **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**





application criticality



Al 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





### **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

Securit Sugge inciden	Security analytics Suggestions for incident response		<b>Threat intelligence</b> Mining, extraction and correlation of information		<b>Vuln. management</b> Discovery of unknown vulnerabilities	
<b>Security analytics</b> Contextualization of incide for investigation	ents	Threat detection Explanation for detections		<b>Risk</b> Automat sec	<b>Risk management</b> Automated assessment of security posture	
Short-term Mid-term			m	Long-term		
Security education Facilitate AI experimentation	<b>Security e</b> Support for se and confi	education ecure coding guration	<b>Vuln. manageme</b> Support for penetra testing	e <b>nt</b> tion	<b>Security analytics</b> Orchestration of complex incident response	
<b>Security education</b> Basic security training	<b>Vulr</b> Disc v	<b>n. management</b> covery of known ulnerabilities	Thre Automa dete	Threat detection Automated definition of detection rules		

### 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 Al technologies, e.g., LLMs gives new opportunity
- Comprehensive report coming up in April!



Applying Artificial Intelligence in Cybersecurity