# Machine Learning & Cybersecurity

Santiago Hernández Ramos @santiagohramos

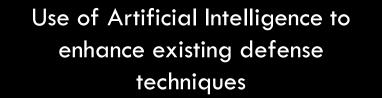
### **CYBERSECURITY AND ARTIFICIAL INTELLIGENCE**

"Al is quickly transforming American life and American business, improving how we diagnose and treat illnesses, grow our food, manufacture and deliver new products, manage our finances, power our homes, and travel from point A to point B."

"Current AI has significant applications in the field of cybersecurity and is expected to play an increasingly important role in both defensive and offensive cyber measures."

https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-Al-Summit.pdf

### **CYBERSECURITY AND ARTIFICIAL INTELLIGENCE**



Use of Artificial Intelligence to enhance existing attack techniques



Santiago Hernández Ramos

## **ARTIFICIAL INTELLIGENCE AND DEFENSIVE SECURITY**



 Machine Learning y Data Science: Curso Completo con

 Python

 Aprende Machine Learning y Data Science con Python, ¡conviértete en un experto en Machine Learning con Python!

 Santiago Hernández

 4,7 ★ ★ ★ ★ (2618)

 31 horas en total · 121 clases · Todos los niveles

 Lo más vendido

🛱 shramos / practical-ml-for-cybersecurity									
<> Code	() Issues	11 Pull requests	🕑 Act	ions 🛄 Projects	🕮 Wiki 🕕 Secu	rity 🗠 Insights 🕸 Se	ettings		
				়িণ্ণ master → ়িণ্ 1 branch 💿 0 tags			Go to file Add file -	⊻ Code -	
				shramos Añadida instalación keras-metrics				a271c76 on 22 May 2020	) 🕚 6 commits
				img		Added colab img			10 months ago
				10_Evaluación	de resultados.ipynb	Commit inicial de los ejercicio	os		10 months ago
				11_Support Ve	ector Machine - Detecci	Commit inicial de los ejercicio	OS		10 months ago
				🗋 12_Árboles de	decisión - Detección d	Commit inicial de los ejercicio	OS		10 months ago

#### **ARTIFICIAL INTELLIGENCE AND OFFENSIVE SECURITY**

Future of Humanity Institute

University of Oxford

Centre for the Study of Existential Risk University of Center for a Cambridge New American Security

a Electronic In Frontier Foundation

oundation

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation February 2018

OpenAI

https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf