www.cybersecitalia.events



4° EDIZIONE BOBBER SECONS

AI, CRITTOGRAFIA POST-QUANTUM, SPIONAGGIO E GEOPOLITICA: IL NUOVO MONDO DELLA CYBERSECURITY

5-6 MARZO

CASERMA SALVO D'ACQUISTO, ROMA



ROMA, 5 - 6 MARZO CASERMA SALVO D'ACQUISTO

RELATORE



ALVARO DEL HOYO MANENE

Southern Europe Technology Strategist, CrowdStrike



www.cybersecitalia.events/cybersec2025 - #CyberSEC2025Rome



ROMA, 5 - 6 MARZO CASERMA SALVO D'ACQUISTO



National Cyber Security Centre

The near-term impact of AI on the cyber threat - NCSC.GOV.UK

The near-term impact of AI on the cyber threat

An NCSC assessment focusing on how AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years.

UK Cyber Policy comment

8/24/24, 7:35 PM

During the Bletchley Al Safety Summit in November 2023, international leaders came together to discuss the vest potential of Al models in promoting economia growth, propelling scientific advances, and providing a wide range of public benefits. They also underscored the security risks that could arise from the irresponsible development and use of Al technologies. The UK government is evaluating and addressing the potential threats and risks associated with Al.

While it is essential to focus on the risks posed by Al, we must also seize the substantial opportunities it presents to cyber defenders. For example, Al can improve the detection and triage of cyber attacks and identify malicious emails and phishing campaigns, ultimately making them easier to counteract.

The Summit Declaration highlighted the importance of ensuring that Alis designed, developed, deployed, and used in a manner that is safe, human-centric, trustworthy, and responsible for the benefit of all. The NCSC continues to work with international partners and industry to provide guidance on the secure development and use of Al, so that we can realise the benefits that Al offers to society, publishing Guidelines for Secure Al System Development in November 2023.

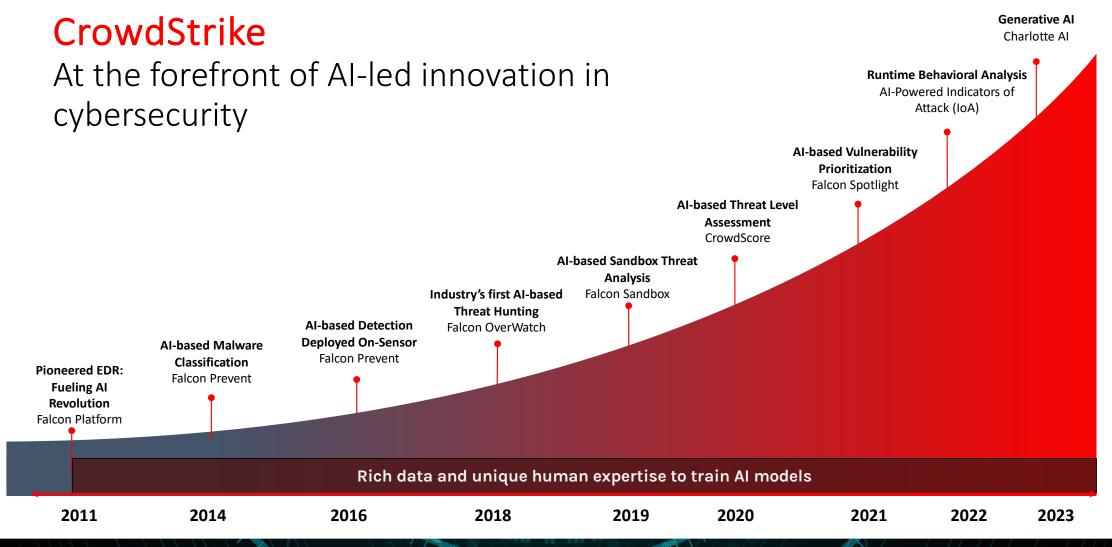
NCSC Assessment

NCSC Assessment (NCSC-A) is the authoritative voice on the cyber threat to the UK. We fuse all-source information – classified intelligence, industry knowledge, academic material and open source – to provide independent key judgements that inform policy decision making and improve UK cyber security. We work closely with government, industry and international partners for expert input into our assessments.

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-th





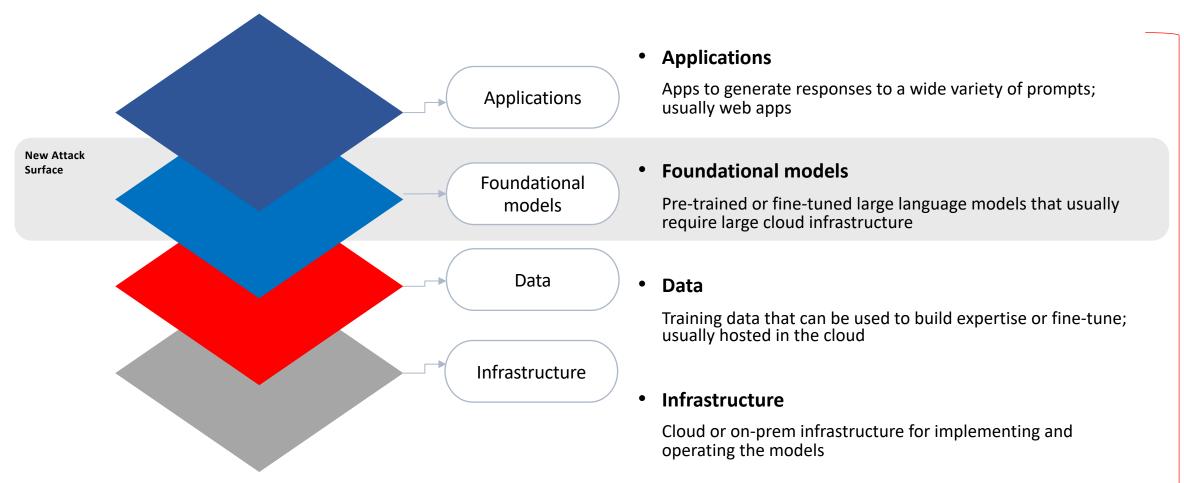


EVENT BY



ROMA, 5 - 6 MARZO CASERMA SALVO D'ACQUISTO

AI Is Part Of Applications That Run On Infrastructure Hosted in a Private or Public Cloud



EVENT BY YBERSECURITY



1

AI, CRITTOGRAFIA POST-QUANTUM, SPIONAGGIO E GEOPOLITICA: IL NUOVO MONDO DELLA CYBERSECURITY

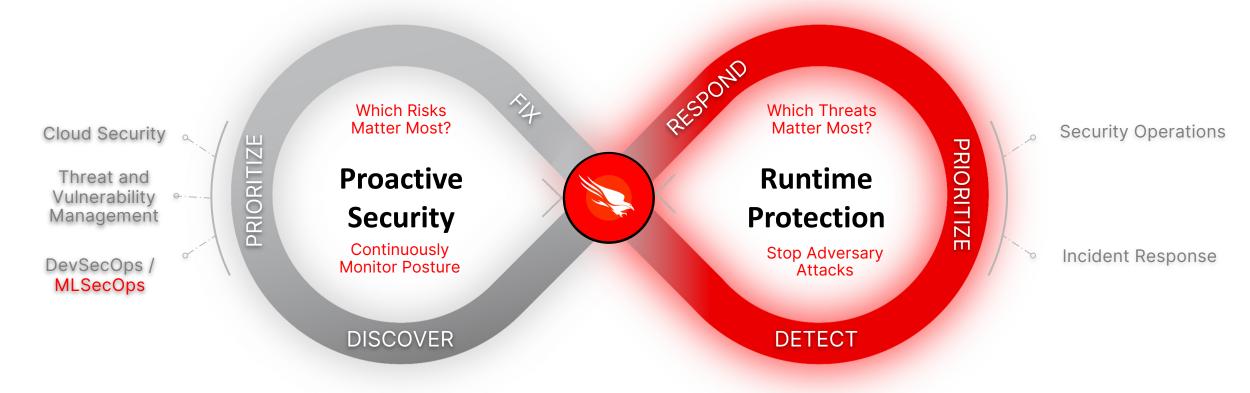
Buying Or Building AI Applications Come With Different Deployment Types And Risks

Buying AI Applications		Building AI Applications			
Consumer Applications	Enterprise Application		Pre-Trained Models	Fine-Tuned Models	Self-Trained Models
3 rd Party Model, Data API or App Access Sanctioned or Not	3rd Party App With Al Features Contractual Relationship Sanctioned		B rd Party Foundation Model wn Workload API integration	3 rd Party Foundation Model Customized Model Own Data Added	1st Party Model Own, New Model Own Data
Shadow AI			3 rd Party Al Risk	1 st ^ 3 rd Party AI Risk	1 st Party AI Risk
 Input & Output Sensitive Data Leakage Contractual Infringement Data Protection Complliance Intellectual Property Reliance On The Unknow 		 Training Data Access Controls Confidential Data, Personal Data For Model Training AI High Risk Processing Contractual Infringement 		 Same as Pre-Trained Models Proprietary Custom Model Own Data Protection 	 Proprietary Model and Training Data Own Data Protection Public IaaS Cloud Service Provider Risk Management
	sk Management			Nanagement →	
Governance 2 Management	Risk 3 Management	Compliance Management	4 Controls Manageme		
		Anaalinaalinaalinaalinaalinaalinaalinaal	gachandhinedizinikanakanakanakanakanakanakanakanakanak		EVENT BY



ROMA, 5 - 6 MARZO CASERMA SALVO D'ACQUISTO

Integrating Security Practices Into AI Applications LifeCycle Management



Flywheel Continuously Hardens Posture to Stop Breaches





ROMA, 5 - 6 MARZO CASERMA SALVO D'ACQUISTO

Get the CrowdStrike 2025 Global Threat Report







CYBERSE-C 2025

GRAZIE!

1 1. Jourthandunahandunahandunahandunahandunahan

alvaro.delhoyo@crowdstrike.com

www.cybersecitalia.events/cybersec2025 #CyberSEC2025Rome