CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts

August 6 2021

I. INTRODUCTION

In response to the European Commission's request for public consultation on Artificial Intelligence, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

A. AI and Machine Learning

The widening adoption of Artificial Intelligence (AI)/Machine Learning (ML) periodically raises fears about automated decision-making, surveillance, algorithmic bias, and other negative externalities. In specific instances, these concerns may warrant suspicion and intense scrutiny. However, it is critical for policy makers to understand that AI/ML also has the opportunity to drive positive social outcomes; is already widely deployed in important instances driving such outcomes; and creates the opportunity for innovation in a variety of important spheres, including industries such as medicine and education.

Our comments will focus on the use of AI/ML within cybersecurity solutions. Legacy cybersecurity solutions used to rely on scanning files against signatures of previously identified malicious files. This process was onerous, resource-intensive, and could be easily circumvented through the use of novel or slightly modified approaches. Next-generation solutions, which leverage AI/ML, can detect previously unknown threats based on their

characteristics or behaviors. This offers much more robust protection against threat activity.

Leveraging AI/ML can achieve success against unknown unknowns. For example, a machine learning model, shipped to CrowdStrike's Falcon Platform customers in September 2019, detected with high confidence the SUNSPOT malware, which was central to a sophisticated campaign that targeted high-value government organizations in late 2020-early 2021.[1] This is one of many instances of AI/ML typifying the best ways to defeat threat actors using new or tailored tools, tactics, techniques, or procedures.

B. AI and Cybersecurity

In cybersecurity, AI is an advantage, especially when added to enterprise security solutions.[2] Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. Indeed, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention.

As such, CrowdStrike recommends that the EC consider exemptions to any future regulations concerning AI. Like in other realms of European Union regulation[3], due to the advantages AI brings to cybersecurity, we encourage the EC to consider a cybersecurity exemption.

Ultimately, CrowdStrike understands that a concern with AI is the possible harm to individuals, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Regulating AI for the sake of the technology rather than its application is not the best approach to foster-innovative solutions to difficult problems. Conversely, we recommend embracing common EU

---

[1] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[2] Michael Sentonas, *How Artificial Intelligence is Becoming a Key Weapon in the Cybersecurity War*, CrowdStrike Blog, Oct. 24, 2017, https://www.crowdstrike.com/blog/how-artificial-intelligence-is-becoming-a-key-weapon-in-the-cybersecurity-war/.

[3] EU regulations regularly acknowledge the unique importance of cybersecurity innovation. The proposed ePrivacy Regulation includes a cybersecurity exemption. Similarly, the General Data Protection Regulation's Recital 49 specifically identifies cybersecurity as a legitimate interest for the processing of personal data.

approaches to protecting the fundamental rights of individuals in a technology-neutral manner. When creating regulations on the safe use of AI, the EC should consider adopting language similar to the General Data Protection Regulation's ("GDPR") requirement that organizations implement safeguards "appropriate" to the risk to protect personal information. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime, 'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

III. CONCLUSION

The EC's proposed regulation provides a thoughtful analysis of a complex legal and policy area. As the EC updates its regulations, we recommend continued engagement with international stakeholders. Adversaries innovate at a record-pace, and it's important to empower defenders to leverage global data flows, big data analytics, and machine learning to protect against ever-evolving threats. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Dr. Christoph Bausewein CIPP/E
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

***