CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

May 13, 2022

I. INTRODUCTION

In response to the European Commission's proposal on the Data Act, 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 hunting, 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

We welcome the European Comission's (EC) data strategy aiming to protect the European Union's (EU) data sovereignty, facilitating the free flow of data within the EU and across sectors to the benefit of businesses, researchers and public administrations, and the controlled and non-discriminatory use of Artificial Intelligence (AI).

A. Principles-Based Frameworks are Future Flexible

One of the main objectives of the Data Act is to help facilitate the free flow of data within the EU. We believe today's economy depends more than ever before on cross-border data flows and data portability. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from anywhere" movement. The importance of cross-border data flows is far-reaching, and affects individuals, entities, and society more broadly. Restrictions on cross-border data flows or overly-burdensome requirements to generate portable

versions of derivative data could have adverse implications for EU innovation, jobs, access to services, and effective cybersecurity. This means that it is critical to provide EU businesses, researchers and public administrations with deference to make their own context-informed—and critically, risk-informed—decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers.

Further, cross-border data flows and unrestricted data portability are necessary elements of some of today's most sophisticated cybersecurity solutions. Many of the most innovative technologies for protecting personal data against data breaches leverage global endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general operates at cloud-scale and invariably involves cross-border data transfers, often involving real-time machine generated event data, derivative analytics, and system-to-system communications.

B. Artificial Intelligence (AI)/ Machine Learning (ML)

The Data Act promotes the non-discriminatory and controlled use of AI. The widening adoption of AI/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 and the EC 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.

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 the EC finalizes the Data Act, it is important to keep flexibility in mind. By this, we mean to emphasize the flexibility of AI as a positive tool in various situations, and not simply an automated-decision making system that could harm the citizens of the EU. We further recommend protecting the rights of EU citizens through a technology-neutral approach. When creating regulations on the controlled and non-discriminatory use of AI, the EC should consider adopting language similar to the GDPR's 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.

---

[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/.

C. Data Re-Use and Access

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. Today, big data analytics provide many benefits, including cybersecurity benefits, due to the ability to re-use data in order to train machine learning models, derive insights over time, and prevent repeat cybersecurity attacks. Embracing this reality is especially important for fulfilling the goals of the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148. Accordingly, it is imperative that the EU's overall Data Strategy and the proposed Data Act align on such outcomes, much in the same way as the recent GDPR guidance issued by the Commission nationale de l'informatique et des libertés (CNIL) issued on the reuse of personal data by processors for their own purposes (adopted January 12, 2022).

In an era of real-time machine generated events, the broad definition of "data" in the proposed Data Act risks making the seemingly-ambiguous obligation to provide data access range from prohibitively expensive and technically burdensome to technically infeasible. GDPR, for example, rightfully draws distinctions between personal data and anonymous data due in part to the potential impact of each data type on an individual. By analogy, and especially in the B2B context, it is important to draw regulatory distinctions between material data provided by or generated about an organization versus derivative data that may be immaterial to the Data User organization but material for a Data Recipient solving a broader problem. In drawing this distinction, the obligation to provide data access becomes one that is technically feasible. Consequently, the aims of the Data Act would be more practically achieved with a narrower definition of "data" and deference provided for B2B relationships to define their own context-specific terms.

D. Cybersecurity Best Practices

The Data Act is but one part of the EC's larger Data Strategy program. Cybersecurity is a key element in achieving the EC's goals of "economic growth, competitiveness, innovation, job creation, and societal progress in general."[3] Below, we offer our views on effective cybersecurity practices.

i. Active Monitoring

[3] A European Strategy for data, European Commission (Feb. 23, 2022), https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

Cybersecurity threats are exceptionally broad, and active monitoring fills an essential role. From our experience, defenders' key responsibility is **threat hunting**. Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organisations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program.

Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the kill chain. Multiple opportunities for detection help avert "silent failures" -- where a failure of security technology results in security events going completely unnoticed.

ii. Remediation & Recovery

Some of the keys to a strong cybersecurity posture today include:

- **Speed**. We advise users that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.

- **Identity Protection and Authentication**: As organisations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services multiply, enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

- **Zero Trust.** Due to fundamental problems with today's widely-used authentication architectures, organisations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

- **Extended Detection & Response (XDR).** 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. The XDR concept seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise, and generate intelligence from what otherwise may be an information overload.

III. CONCLUSION

The Data Act is cited as being the "pillar for European strategy for data" with the objectives of "harnessing the potential of the ever-increasing amount of industrial data, in order to benefit the European economy and society."[4] To achieve this, we recommend the EC consider the implications of unintended incentive structures that may be created by overly-broad and ambiguous definitions. Ultimately, it is critical to prioritize future-flexible data flows, as well as the flexibility to solve not

[4] A European Strategy for data, European Commission (Feb. 23, 2022), https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

only the problems of today, but to realize the innovative potential of tomorrow. Finally, we emphasize the importance of cybersecurity best practices.

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, CIPT
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

***