REQUEST FOR COMMENT RESPONSE

Cyber Solidarity Act

July 20, 2023

I. INTRODUCTION

In response to the European Commission's ("Commission") request for feedback on the proposed Cyber Solidarity Act ("CSA"), 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 organisations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate the Commission's efforts to improve the cybersecurity of the European Union ("EU") by strengthening capacities to "detect, prepare for and respond to cybersecurity threats and incidents."

The Commission appropriately notes that cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a notable surge in identity-based threats and cloud exploitations. Further, we found a 112% year-over-year increase in advertisements on the dark web for identity and access credentials, a 95% increase in cloud exploitation by threat actors, over 30 new adversaries, and numerous new ways that eCrime actors weaponize and exploit vulnerabilities.[1] As adversaries continue to evolve and find new ways to target victims, organisations must increase their emphasis on cybersecurity practices that leverage the most effective technologies.

[1] *CrowdStrike Global Threat Report*, 2023. https://www.crowdstrike.com/global-threat-report/

While we do not have feedback on every aspect of the proposed Act, we do want to offer several points that may be of value to the Commission as it considers the proposed Act.

A. Information Sharing is Key for Cybersecurity

The Commission captures the correct sentiment that data and information shared in a safe manner leads to more accurate and actionable cyber threat intelligence. The CSA proposes creating the European Cyber Shield – to detect, analyse, and process data on cyber threats across the EU – made up of National Security Operation Centres ("SOCs") and Cross-border SOCs. The CSA outlines that the European Cyber Shield will share data on cyber threats and incidents from various sources, produce threat intelligence using tools such as Artificial Intelligence ("AI"), and provide cybersecurity services across the EU.

However, for the European Cyber Shield to be effective, the emphasis on information sharing across countries must be upheld during the implementation. Unfortunately, across the EU there are examples of countries imposing data localization requirements, for supposed data protection objectives, that are counterproductive and actually end up lowering cybersecurity capabilities which leads to a decreased ability to protect data.[2] A few examples of these measures include France's draft cybersecurity certification, SecNumCloud,[3] an early draft of Italy's Presidential Decree implementing NIS 1.0,[4] certain interpretations of post-Schrems II cross-border data flows, and other policies promoting data sovereignty for domestic intelligence gathering, industrial policy objectives, or as a misplaced proxy for cybersecurity.[5] As a leading cybersecurity provider, it is our view that perhaps the most significant threat to data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules, so

---

[2] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479.

[3] *Cloud Computing Service Providers (SecNumCloud) Requirements*, 2022.
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf

[4] *Regulation on notifications of incidents having an impact on networks, information systems and information services*, 2019.
https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

[5] *Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance*, 2023.
https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance/

national laws should focus on stopping data exfiltration by bad actors rather than localisation requirements that will not be followed by adversaries.

Research has shown that data localization can have an adverse impact to cybersecurity and restricts the ability of defenders to follow best practices.[6] In order for the European Cyber Shield to accomplish its goal of sharing data on cyber threats multinationally, data must be shared across the EU and with other partner countries.

B. Leverage Partnerships

The EU should leverage international partnerships with the private sector to defend against cybersecurity attacks. The EU Cybersecurity Reserve is the CSA's service that may be deployed to Member States to assist during significant cybersecurity attacks. The Commission will leverage trusted cybersecurity providers to make up the offerings of the EU Cybersecurity Reserve. The Commission should select the best cybersecurity technologies and providers, no matter which like-minded country they are headquartered, that are best equipped to assist and remediate during a cybersecurity attack.

In some cases, best-in-class cybersecurity providers may also be helpful in building the infrastructure and protections for the National and Cross-border SOCs in the European Cyber Shield. Sophisticated countries gather threat intelligence within their country and from any multinational agreements; however, countries can benefit from supplementing their threat intelligence with private sector enterprises which have additional knowledge and insights from processing global cyber events day-to-day on a large scale. For example, CrowdStrike's highest-fidelity security data includes the trillions of security events captured in the CrowdStrike *Threat Graph* daily, asset telemetry from across users, devices, identities, cloud workloads, and threat intelligence, to drive efficacy and actionability.

Finally, the CSA wants to use AI to boost cybersecurity practices. We applaud the CSA's inclusion of AI for cybersecurity as we view leveraging AI for cybersecurity as a best practice. CrowdStrike has deployed AI at scale across tens of millions of endpoints for prevention, dating back ten years. Other vendors are also experimenting with these

---

[6] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479

tools. The Commission should leverage private-sector leaders who have experience using AI to supplement cybersecurity in the implementation of the CSA.

C. Engage Countries Outside of the EU

Like in other realms of public safety, including the example set forth by Europol's EC3, the EU can benefit from like-minded countries participating in the European Cyber Shield and sharing information, when appropriate, if they meet the security requirements set out in Article 8. As mentioned above, the more data points gathered across the globe, the more accurate threat intelligence can be produced. Additionally, if the European Cyber Shield expands to include the private sector, the Commission should look at best practices and lessons learned from the United State's Joint Cyber Defense Collaborative (JCDC) which has been a key development in promoting information sharing and collaboration. JCDC has created a platform for key players in industry and government to voluntarily work toward common goals and it may serve the EU to follow a similar model.

III. CONCLUSION

The Commission's proposed regulations provide a thoughtful analysis of a complex legal and policy area. As updates to the CSA move forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasise that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

Throughout this effort, the EU should not lose sight of the objectives pursued in the Commission's Digital Strategy of 2022 addressing the EU's digital transformation opportunities, and supporting the delivery of the EU's strategic priorities that focus on improvements to the EU's cyber-resilience by 2030.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, 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/.

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

Elizabeth Guillot
Manager, Public Policy

Email: policy@crowdstrike.com

***