REQUEST FOR INFORMATION RESPONSE

National Priorities for Artificial Intelligence

Docket ID: OSTP-TECH-2023-0007

July 7, 2023

I. INTRODUCTION

In response to the Office of Science and Technology Policy's ("OSTP") request for information ("RFI") to develop a National Artificial Intelligence Strategy, 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 appreciate the OSTP's efforts to create a comprehensive national strategy on Artificial Intelligence ("AI"). The request for information correctly notes that AI is evolving at a rapid pace and creating benefits, and considerations of risks, across many sectors and aspects of life. The cybersecurity sector is no different with AI enhancing security capabilities while also creating new threats that require mitigation.

While we do not have feedback on every question in the RFI, we do want to offer several points that may be of value to the OSTP as it drafts the National AI Strategy.

A. *Question* 4) What are the national security benefits associated with AI? What can be done to maximize those benefits? **AND** *Question* 6) How can AI rapidly identify cyber vulnerabilities in existing critical infrastructure systems and accelerate addressing them?

Cyber threat actors are constantly evolving and finding new ways to target victims, including private sector entities and government agencies involved in national security. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a notable surge in identity-based threats, cloud exploitations, and malware-free attacks. Adversaries continued to move beyond malware to gain initial access with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021); a contributing factor to this was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits. Further, we found 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, organizations must increase their emphasis on cybersecurity practices that leverage the most effective technologies, AI being one of those.

The use of AI to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks, because AI can defeat novel threats based on behavior cues rather than known signatures. Leveraging these technologies is essential to meeting constantly-evolving threats.

While the public discourse around AI has grown exponentially in the last year, AI in cybersecurity is not a new concept. 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 tools. As a community, we should continue to leverage AI for cybersecurity use cases.

B. *Question* 5) How can AI, including large language models, be used to generate and maintain more secure software and hardware, including software code incorporating best practices in design, coding and post deployment vulnerabilities?

Across the cybersecurity, software development, and broader high technology ecosystems, significant experimentation with AI is taking place. This experimentation is

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

likely to yield some security improvements within the software and hardware development and validation spaces. Further, the application of AI to optimizing existing software or better securing existing platforms is an important opportunity.

For example, CrowdStrike leverages LLMs to assist analyst workflows and to make other security analyst tasks more efficient. This capability (coined "*Charlotte*") utilizes CrowdStrike's highest-fidelity security data, which includes the trillions of security events captured in the CrowdStrike Threat Graph, asset telemetry from across users, devices, identities, cloud workloads, and threat intelligence. The use of this knowledge base drives efficacy, actionability, and relevance, as well as addresses the risk of "hallucination."

Further, the natural language interface seeks to make cybersecurity responsibilities more broadly accessible. Our goal with *Charlotte* is to help close the cybersecurity skills gap and improve the response time so users can stay ahead of adversaries – boosting security across organizations. Today, we see this use of LLMs as one of the most relevant to improving security outcomes in the near- to mid-term.

C. *Question 19*) What specific measures—such as sector-specific policies, standards, and regulations—are needed to promote innovation, economic growth, competition, job creation, and a beneficial integration of advanced AI systems into everyday life for all Americans? Which specific entities should develop and implement these measures?

From our vantage as a cybersecurity company, the cybersecurity workforce has a role to play in the innovation and growth of AI–and vice versa (See answer 'B,' above). We recommend that the National AI Strategy align with the forthcoming Cybersecurity Workforce Strategy, from the Office of the National Cyber Director's (ONCD), in whatever ways are practical. CrowdStrike previously commented on the ONCD *Request for Information on Cyber Workforce, Training, and Education* and noted many of the steps we are taking towards both increasing the number of people in the cyber workforce and ensuring the cyber workforce is diverse and inclusive.[2]

[2] CrowdStrike comments on the ONCD *Request for Information on Cyber Workforce, Training, and Education*, 2022.
https://www.crowdstrike.com/wp-content/uploads/2023/02/Cybersecurity-Workforce.pdf.

D. *Question* 28) What can state, Tribal, local, and territorial governments do to effectively and responsibly leverage AI to improve their public services, and what can the Federal Government do to support this work?

State, local, Tribal, and territorial (SLTT) governments should consider acquiring cybersecurity technologies that leverage AI to bolster their security. Where these technologies offer superior defense against threats such as ransomware and data extortion, public services will remain more robust and citizens' privacy will be better protected. As the White House noted in the ONCD *Request for Information on Cyber Workforce, Training, and Education*, SLTT governments, like federal agencies, face the same challenges in finding cyber talent to implement substantial cybersecurity programs that appropriately defend against the threat landscape.[3] SLTT governments can leverage managed service providers (MSPs) to carry out their cybersecurity programs, using best-in-class technologies, often for significantly less cost than hiring for and building a security program. The Federal Government can continue to support this through grants – such as the State and Local Cybersecurity Grant Program established by the Infrastructure Investment and Jobs Act of 2021[4] – and funding mechanisms that include MSPs as appropriate use of funds.

III. CONCLUSION

The OSTP's RFI provides a thoughtful analysis of a complex, constantly evolving, policy area. As the National AI Strategy moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the strategy focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

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

[3] ONCD *Request for Information on Cyber Workforce, Training, and Education*, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/ONCD-Workforce-and-Education-RFI.pdf.

[4] https://www.cisa.gov/state-and-local-cybersecurity-grant-program.

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

***