EUROPEAN ACTION PLAN ON THE CYBERSECURITY OF HOSPITALS AND HEALTHCARE PROVIDERS

June 30, 2025

I. INTRODUCTION

In response to the European Commission's ("Commission") consultation on the European action plan on the cybersecurity of hospitals and healthcare providers ("Action Plan") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, AI-native, 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

CrowdStrike supports the Action Plan's goal of better protecting hospitals, healthcare providers and citizens from cybersecurity threats. As the Commission knows, healthcare is unfortunately one of the most heavily-targeted critical infrastructure sectors. Cyber threat actors attempt to breach healthcare entities for a variety of reasons based on their different motivations. Cyber criminal (eCrime) actors seek to monetize hacking these entities through ransomware, data extortion, Business Email Compromise (BEC), theft of medical records, and access to banking and payment information. Nation-state actors target the sector seeking information about specific individuals or broad populations for espionage purposes, and could leverage disruptive or destructive attacks to advance geopolitical aims. "Hacktivist" actors may also target entities in the sector, directly or inadvertently, to advance a social or political advocacy agenda.[1]

[1] "*Examining Health Sector Cybersecurity*," CrowdStrike Testimony, April 16, 2024. https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/evo-media-document/Robert%20Sheldon_Witness%20Testimony_04.16.2024.pdf.

These threats continue to evolve and grow more severe. CrowdStrike's latest Global Threat Report notes that interactive intrusion activity against the healthcare sector continues to be significant, with 9% of tracked intrusions targeting the sector in 2024.[2] Additionally, in 2024, China-nexus activity surged 150% and common eCrime technique "Vishing" attacks skyrocketed 442% between the first and second half of 2024 across all sectors – making steps to enhance cybersecurity in the sector timely and appropriate.

While we do not have feedback on every aspect of the Action Plan, we do want to offer several points that may be of value to the Commission.

A. Cybersecurity Risk Management Practices

We commend the Commission for recognizing the changed environment for healthcare and the need to strengthen cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture that should be included in the Action Plan's future targeted guidance of cybersecurity best practices. The Action Plan discusses the benefit of some of today's most effective cybersecurity practices. We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

Organizations should leverage several key technologies to defend against cyber threat actors:

- **Cloud Security**. Leveraging cloud systems provides numerous operational efficiencies and security enhancements, and as the Action Plan notes, the majority of health organizations are leveraging cloud-based digital health platforms for these benefits. Given today's rapidly evolving threat landscape, organizations must address cloud-specific and cross-domain threats (where adversaries traverse cloud and on-premise environments). Security teams must protect data, manage identity and access, and hunt for and respond to threats in real-time. Capabilities of particular relevance include cloud workload protection, cloud-native application protection platform (CNAPP), cloud security posture management (CSPM), and Software-as-a-Service (SaaS) security.

[2] An interactive intrusion occurs when threat actors perform hands-on-keyboard activities within a victim's environment; as opposed to a bot or spam. Interactive intrusions, or hands-on-keyboard attacks, are typically more sophisticated and difficult to detect compared to automated attacks, requiring advanced threat hunting and incident response capabilities to identify and mitigate. "2025 *Global Threat Report*," CrowdStrike, https://www.crowdstrike.com/en-us/global-threat-report/.

- **Endpoint Detection and Response (EDR)**: EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs.

- **Next-Generation Security Information and Event Management (SIEM) solutions.** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by EDR tools) and integrate it with other security-relevant event information from an array of sources. Supported by AI, this provides defenders a more coherent view, intuitive workflows, and ultimately better control of their environments.

- **Artificial Intelligence (AI)-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. AI and machine learning are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **Identity Threat Detection and Response (ITDR)**: As organizations increase deployment of cloud services, work from anywhere models, and Bring-Your-Own-Device policies, enterprise boundaries continue to erode. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. In fact, compromised valid identities are a common initial access vector in incidents. However, emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should consistently measure and reduce their response time.

- **Threat Hunting**. The Action Plan rightfully places an emphasis on the unique threats the health sector faces and the need to leverage threat intelligence to stay ahead of the adversary. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year.

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. The Action Plan notes that MFA is a basic requirement to protect entities from identity and credential theft attacks. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Security Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally, or lack the scale to

support a robust, 24/7, 365 days per year security capability. Increasingly, such entities should rely upon managed service providers, which can be more efficient overall and enable organizations to apply internal IT/security resources toward domain-specific challenges, including governance, risk, and compliance. Adopting an MSSP can radically strengthen organizations' security posture. CrowdStrike supports the "Cybersecurity Vouchers" idea raised in the Action Plan that requests Member States consider financial assistance for micro, small, and medium-sized hospital and healthcare providers to put in place external cybersecurity measures.

Relatedly, the Action Plan recommends cloud services use secure development practices. CrowdStrike views Security-by-Design and -Default principles as a positive change in driving greater security accountability for product makers.

B. Maturity Assessment

The Action Plan tasks the Support Centre to develop a tailored framework for cybersecurity maturity assessments specific to healthcare. The goal of the maturity assessments would be to provide entities with actionable insights into their vulnerabilities while allowing them to demonstrate their cybersecurity readiness to patients and stakeholders, building trust in their services. The fundamental question of a maturity assessment is "how effectively does the security program address the cyber risks the organization faces?" Flexible frameworks are ideal for this type of evaluation as maturity assessments need to be tailored for the organization completing it. The best maturity assessments should combine the types of security measures but place them in an operational context—both in terms of what threat actors are likely to exploit and what defenders can realistically accomplish.

Maturity assessments are an internal exercise, often done under client privilege with a third-party firm, and businesses should not be required to submit assessments to the Commission.

C. Support Centre Engagement with Private Sector

The Action Plan calls for the Commission to create an European Cybersecurity Support Centre specifically for hospitals and healthcare providers to carry out many of the directives in the Action Plan. For the goals of the Support Centre to be met, engagement with the private sector is essential. For example, the action items to: 1)

address significant challenges of threat detection creating an EU-wide early warning subscription service for the health sector to deliver near-real-time alerts; 2) enhance the EU Cybersecurity Reserve to include a Rapid Response Service specifically for the health sector; and 3) create a Health Cybersecurity Advisory Board with opportunities for commitments to best practices from relevant organizations, must include ample collaboration with private sector cybersecurity organizations in order to be successful. The Support Centre should leverage the private sector especially where private organizations have developed technologies, best practices, and solutions for the problems the Support Centre is tasked to solve - such as threat intelligence and incident response.

Additionally, we support the placement of such a support centre in ENISA, provided that the upcoming EU Cybersecurity Act addresses the resourcing needed for ENISA to add this Centre to its responsibilities.

D. Artificial Intelligence

The Action Plan describes the benefits AI can bring to the healthcare sector such as addressing the shortage of healthcare professions and improving cybersecurity functions. 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 best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats and the goals of the Action Plan.

III. CONCLUSION

The Action Plan represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the healthcare sector uses strong cybersecurity practices due to the amount of sensitive data they protect and the regulations to which they are subject. With an emphasis on adoption of practical security practices, these new requirements and programs can raise the already high standard of cybersecurity in the healthcare sector. As the Commission moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

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

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***