CROWDSTRIKE RESPONSE TO THE EUROPEAN COMMISSION CALL FOR EVIDENCE ON THE REVISION OF THE EU CYBERSECURITY ACT

20 June 2025

I. INTRODUCTION

In response to the European Commission's ("Commission") Call for Evidence on the revision of the EU Cybersecurity Act ("CSA") 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

The EU's vision for achieving better resilience with the revision of the CSA depends fundamentally on principles of a secure digital ecosystem. Europe's ambition to strengthen resilience can be significantly increased by embracing collaboration with trusted international technology providers. Many global companies, including CrowdStrike, actively support Europe's digital ecosystem fully complying with EU regulations such as the Network and Information Security Directive 2 ("NIS 2"), Digital Operational Resilience Act ("DORA"), the Cyber Resilience Act ("CRA") and General Data Protection Regulation ("GDPR"). Recognising and building on these contributions through supportive policy frameworks will help ensure that European users benefit from cutting-edge innovation and secure, high-quality IT solutions.

III. RECOMMENDATIONS

We support the Commission's vision to clarify the mandate of the EU Agency for Cybersecurity ("ENISA"), and improve the European Cybersecurity Certification Framework ("ECCF"). We also support the aim to streamline, simplify and supplement EU legislation to make the implementation of the ECCF more user and business

friendly and to prioritise measures to support the EU objectives of developing a secure and resilient supply chain. We welcome the opportunity to offer several points that may be of value to the Commission as it revises the CSA.

A. *Mandate of the EU Agency for Cybersecurity* ("ENISA")

ENISA has been instrumental in providing the critical interaction between the public and private sectors on the rapid development and needs of the EU on cybersecurity. We support the continued development of strategic partnerships with global cybersecurity vendors, industry ISACs, standards bodies (e.g. ETSI, ISO, NIST), and research institutions to best address in advance various guidelines and implementation of all current and upcoming cybersecurity related acts. The evolving cyber threat landscape demands that ENISA is able to consult with the private sector to maintain and expand its role as an operational cornerstone of European cyber resilience.

B. *Improving the ECCF: Advancing Risk-Based, Flexible Cybersecurity Certification*

CrowdStrike supports the overarching goal of the ECCF to establish a unified, transparent, and technically sound approach for certifying ICT products, services, and processes. By promoting harmonisation across Member States, the ECCF can play a pivotal role in reducing market fragmentation, enhancing trust in digital technologies, and strengthening the cybersecurity resilience of the EU as a whole.

We acknowledge the progress made under the ECCF, notably the adoption of the European Common Criteria-based certification scheme. Common Criteria (ISO/IEC 15408) has historically served as a global benchmark for cybersecurity assurance and remains valuable in certain contexts. However, the evolving threat landscape and rapid technological innovation require certification schemes—especially those grounded in legacy methodologies—to continuously adapt.

Certification must evolve to account for:

- Rapid adversary innovation and increasingly sophisticated threat techniques;
- Modern cloud-native and distributed architectures; and
- Ephemeral endpoints and agile development cycles underpinning digital transformation.

To ensure ECCF schemes remain effective and relevant, CrowdStrike recommends promoting a principle-based, risk-driven certification approach. CrowdStrike cautions

against rigid, overly prescriptive technical standards in certification design. While harmonised rules provide legal certainty, fixed technical criteria may quickly become outdated, undermining their value in a fast-changing environment. Prescriptive schemes risk creating a *compliance-first mindset* where adherence to static checklists eclipses the goal of achieving meaningful, real-world security. This concern is especially acute for small and medium-sized enterprises (SMEs) that face disproportionate administrative burdens and managed security service providers (MSSPs) delivering high-velocity, adaptive services such as incident response, threat intelligence, and real-time monitoring.

We urge the Commission to pursue revising the ECCF framework to develop a *principle-based*, *outcome-oriented* model that allows certifications to be:

- Tailored to evolving threat models;
- Responsive to new operational and technological realities; and
- Periodically reviewed, updated, or retired to avoid staleness and maintain relevance.

C. *Aligning ECCF to Best Practices*

To maintain credibility and operational value, cybersecurity certifications must align with evolving best practices. These include:

- **Cloud Security**. Leveraging cloud systems provides numerous operational efficiencies and security enhancements. 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.

- **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 Endpoint Detection and Response [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.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence 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**. 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 security protections focused on identity and authentication. By eliminating transitive trust, Zero Trust Architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats.

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

- **Managed Security Services** 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 MSS can radically strengthen organizations' security posture.

D. *Build Fit-for-Purpose Certification for Managed Security Services*

Certification can improve trust in Managed Security Services (MSS), especially in high-risk or critical sectors. However, applying certification uniformly across all MSS categories risks overregulation. Therefore:

- **Risk-Based Assurance Levels**: The defined assurance levels ("basic," "substantial," and "high") should reflect the unique risk profiles and attack surfaces of MSS, rather than being automatically imposed. For example, real-time threat intelligence services should not be subject to the same certification regime as managed infrastructure services unless risk-justified.

- **Avoid Blanket Mandates**: Certification should only be made mandatory for MSS where clear risk assessments and multi-stakeholder consultation demonstrate a need. Imposing certification indiscriminately would stifle innovation and disrupt service delivery, particularly in agile fields like incident response or AI-assisted threat hunting.

- **Support for Modular, Scalable Certification**: The ECCF should accommodate the dynamic and modular nature of MSS. Certification schemes must account for frequent updates, service customisation, and cloud-native or AI-enabled architectures. Agile certification pathways would promote adoption while maintaining technical integrity.

Due to the existing multiple step verification and approval process foreseen in the CSA, a simplification of the ECCF to ensure a technocratic process should considerIncreased transparency and opportunities for public consultation. The current ECCF has one opportunity for a public consultation before the candidate scheme is drafted, however once the candidate scheme is passed on from the ENISA ad hoc working group and receives the opinion of European Cybersecurity Certification Group (ECCG), there is no longer an opportunity to give feedback on the scheme. Due to the rapidly developing technology being certified, maximum transparency on the drafting process should be considered as well as multiple opportunities to provide input as the draft scheme circulates between ENISA and the ECCG.

D. *Streamline, simplify and supplement EU legislation to make the implementation of the ECCF more user and business friendly*

The aim to streamline, simplify and supplement EU legislation including its regulatory instruments and the ECCF should actively promote regulatory harmonisation and coherence across Member States and among overlapping legislative frameworks such as the CSA, CRA, GDPR, NIS2, DORA, the Digital Services Act, the Artificial Intelligence Act, and sector-specific laws (e.g. the Medical Devices Regulation). Today's fragmented

and overlapping regulatory environment creates uncertainty, increases compliance burdens, and risks deterring adoption of effective cybersecurity measures—especially among Small and Medium Enterprises (SMEs), startups, and sectors with limited digital maturity.

To ensure the EU builds and sustains its cybersecurity advantage in an era of accelerating digital and AI-driven threats, both public and private sectors must be empowered to innovate. New regulations or certification schemes must not inadvertently stifle the development or deployment of security-enhancing technologies. Security should be measured by outcomes, not compliance alone. Regulating cybersecurity tools or practices based on their category—rather than their function and real-world impact—risks slowing the EU's response to increasingly agile and well-resourced adversaries. To stay ahead, organizations must be encouraged to adopt and integrate advanced cybersecurity practices, including those that leverage AI and automation, as a central element of their defense strategy.

E. *Prioritisation of measures to support the EU objectives of developing a secure and resilient supply chain*

CrowdStrike strongly supports the EU's objective of developing a secure and resilient digital and cybersecurity supply chain. A trustworthy and robust supply chain is foundational to EU cybersecurity, digital sovereignty, and the broader success of the Digital Single Market. To achieve this, CrowdStrike recommends a prioritised approach grounded in risk management, flexibility, innovation, and cross-sectoral partnership.

A critical foundation of this effort is the development of **risk-based, outcome-oriented certification frameworks**. CrowdStrike advocates for certification schemes that are principle-based rather than prescriptive, ensuring they align with real-world threat models and evolving adversary tactics. Static, checklist-driven approaches risk becoming obsolete and may fail to capture the dynamic nature of current threats. Certification frameworks must support agile and modular pathways, particularly as organisations adopt modern architectures and cloud-native solutions. A flexible approach to certification will build trust without constraining innovation, and is especially important for small and medium-sized enterprises operating in fast-paced environments.

CrowdStrike also emphasises the importance of **secure-by-design and secure-by-default product development**. To reduce vulnerabilities across the supply

chain, product manufacturers must prioritise eliminating recurring classes of vulnerabilities. Security should be embedded throughout the product development lifecycle—not bolted on afterward. Additionally, prioritising usability and transparency for end users will encourage broader adoption of secure products and create positive market incentives for responsible development practices.

IV. CONCLUSION

In conclusion, CrowdStrike supports the ECCF's objectives and encourages the European Commission to refine certification practices to reflect real-world threats, accommodate modern service models, and avoid one-size-fits-all mandates. A flexible, risk-based, and innovation-friendly ECCF will better protect EU interests, empower industry, and strengthen collective cyber resilience.

CrowdStrike supports the EU's vision of a secure digital future and believes the development of a resilient cybersecurity supply chain must be rooted in real-world risk, adaptable certification, and forward-looking design. By prioritising security from the ground up and encouraging flexible, scalable solutions, the EU can lead in setting high cybersecurity standards while fostering innovation and resilience across its digital ecosystem.

V. 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/.

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

Līga Rozentāle, CISM
Director, Public Policy EU/International

Email: policy@crowdstrike.com

###