CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)

May 19, 2022

I. INTRODUCTION

In response to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) request for feedback on the Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA), 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

The SCuBA project's stated objectives, to "*provide architecture and security configurations that offer fundamental protections for cloud business applications and give [Federal Civilian Executive Branch] FCEB agencies and CISA the visibility necessary to identify and detect adversarial activity in their cloud environments*," is timely and essential. From a threat perspective, CrowdStrike increasingly sees threat actors across multiple motivations targeting cloud workloads.[1] FCEB entities, some of which remain in the early phases of migration to cloud and Software-as-a-Service (SaaS) offerings, must adopt robust cloud security practices that promote visibility, detection, and response.

[1] See, for example, https://www.crowdstrike.com/global-threat-report/.

We note that "*the management and security of the endpoints are outside the scope of the SCuBA TRA.*" Nevertheless, we appreciate references in the document to resources that address those issues, such as the *CISA Cloud Security Technical Reference Architecture* and the *CISA Zero Trust Maturity Model*, which address those essential topics in detail. We refer reviewers to comments CrowdStrike previously submitted on those documents (both dated 1 October 2021). The draft TRA further states that:

> *Managing endpoints (both mobile and desktop) is critical to securing cloud business applications and to support a [Zero Trust] ZT approach.*

To this end, we strongly encourage CISA to design endpoint security initiatives that can achieve comprehensive visibility and streamlined detection and response across varied endpoints. Defenders should have a unified view of threats targeting all types of endpoints—whether laptop, desktop, server, mobile, or cloud workload. This is preferable because:

- **Workloads change as new technologies are deployed and legacy infrastructure is modernized**. Using different detection and response systems may mean defenders' visibility is adversely impacted as technologies evolve (e.g., an application previously accessible exclusively through workstations becomes available via mobile app.)

- **Adversaries pursue different attack surfaces/targets during a single campaign.** Comprehensive visibility, with common reporting schemes/language, can enable defenders to quickly identify the scope/severity of a broad campaign targeting an FCEB entity. Partial visibility or different reporting complicates defenders' ability to understand the extent of ongoing threat activity.

- **Adversaries move laterally between endpoints during attacks**. To the extent that disparate solutions are unnecessarily used to defend different technology categories/environments, defenders may expect reduced ability (or lack the ability) to create easily understable *attack narratives* that describe breach conditions during investigations and remediations.

III. CONCLUSION

The draft TRA provides thoughtful analysis and guidance for a complex and evolving technology area. To provide the most robust possible defenses to FCEB entities, we encourage CISA to adopt as comprehensive an approach as possible to visibility, detection, and response. We welcome the opportunity to engage further on these topics.

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

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***