Secure Cloud Business Applications Frequently Asked Questions

October 2022

WHAT IS SCUBA?

The Secure Cloud Business Applications (SCuBA) project provides guidance and capabilities to secure agencies' cloud business application environments and protect federal information created, accessed, shared, and stored within those environments.

WHY IS SCUBA IMPORTANT?

The SCuBA project enables the Cybersecurity and Infrastructure Security Agency (CISA) to provide protection and visibility guidance into the cloud environments of federal civilian executive branch (FCEB) agencies per authorities granted in the 2021 National Defense Authorization Act. SCuBA will enhance the security of FCEB cloud business application environments through strong configurations, settings and security products. This project accelerates CISA's cybersecurity shared services development and strengthens its ability to drive security improvements across the FCEB.

WHAT ARE THE VARIOUS WORKSTREAMS?

CISA published two guidance documents and will soon release product-specific security configuration baselines as a part of a concerted effort to help agencies leverage best practices for cloud software as a service security:

- The SCuBA Technical Reference Architecture (TRA) is a security guide that agencies may use to adopt technology for cloud deployment, adaptable solutions, secure architecture, agile development, and zero trust frameworks.
- The Extensible Visibility Reference Framework (eVRF) Guidebook provides a framework overview, which allows agencies to identify visibility data for use in mitigating threats. The EVRF also helps organizations identify potential visibility gaps.
- The SCuBA team is developing product-specific security baselines for critical business applications within the Microsoft 365 (M365) and Google Workspace (GWS) cloud productivity suites. These baselines will provide agencies with information on both baseline security configurations and additional enhancements to bolster their security. Product-specific security baselines have also gone through a rigorous testing period, including penetration and Risk and Vulnerability Assessment testing.

Collectively, these SCuBA guidance documents will help agencies adopt necessary security and resilience practices when utilizing cloud services.

WHEN WILL CISA LAUNCH SCUBA?

CISA will launch a test pilot in FY23 to examine product-specific security baselines implementation for M365. As the SCuBA project progresses, CISA will determine potential candidate cybersecurity shared service offering(s) in support of secure cloud business applications.

HOW MUCH WILL SCUBA COST AGENCIES?

SCuBA guidance and consultation surrounding implementation for the pilots is available at no cost to agencies. Agencies will need to supply personnel hours for application of the proper configuration settings within their respective environments; however, automation efforts are under development and should be completed soon to ease the workload associated with implementation of the baselines.

HOW WILL CISA WORK WITH AGENCIES?

- SCuBA's guidance documents—the SCuBA TRA, eVRF Guidebook, and product-specific security baselines for both M365 and GWS—will provide agencies with blueprints to secure their cloud business applications. While FCEB agencies are the main target, CISA's guidance will also be instructive for other entities, including private-sector partners; owners and operators of National Critical Functions (NCFs); and state, local, tribal and territorial (SLTT) governments. Notably, these guidance documents were developed with interagency input and consultation.
- After months of developmental work, CISA is releasing a series of Security Configuration Baselines for M365 as part of its SCuBA project. The CISA documents build on M365 security configuration baselines developed by the Federal Chief Information Officers (CIO) Council's Cyber Innovation Tiger Team (CITT).
- As a part of the project plan, the SCuBA team will be piloting visibility, configuration, and security-hardened product-specific security baselines with selected FCEB agencies. That pilot will allow FCEB agencies the opportunity to provide hands-on feedback on guidance implementation.

HOW WILL CISA WORK WITH INDUSTRY PARTNERS?

There have been Requests for Information, comment periods, interviews, and engagements with stakeholders throughout SCuBA that will continue as the project progresses.

WHAT ARE THE NEXT STEPS?

CISA will finalize guidance documents, including the SCuBA TRA, eVRF Guidebook and product-specific security baselines. These foundational pieces of guidance will be critical for FCEB agencies and instructive for other entities. However, CISA is also ensuring that guidance is practicable for implementation. CISA will work with FCEB agencies to pilot configuration recommendations within the product-specific security baselines, along with the role of automation in their implementation.