HPE ARUBA NETWORKING FEDERAL SYMPOSIUM

Secure Cloud Business Applications (SCuBA)

Chad Poland – Capacity Building, Cybersecurity Shared Services Office(CSSO), Cybersecurity Division (CSD), CISA, DHS

SCuBA Overview

Cloud Solutions Architecture

- SCuBA **develops architecture implementation guidance for cloud solutions** to centralize and simplify planning and implementation guidance.
- The **Hybrid Identity Solutions Architecture, Technical Reference Architecture**, and **Secure Web Gateway** guidance are in various stages of development.

Engagements

- Agency pilots **exercise SCuBA's guidance and tooling** in an agency's environment to address issues with security and functionality.
- Workshops **build the capacity** for an organization's use of SCuBA's tools and guidance by **collaboratively engaging** agencies with technical expertise.
- Technical Exchange Meetings bring together key stakeholders to identify areas for continuous **product improvement and future service offerings**.

Secure Configuration Baselines

- SCuBA is developing **product-specific guidance** for Microsoft 365 and Google Workplace on how to configure agency cloud environments to their full security potential.
- **Automated assessment tools** provide an easily digestible, visual report to identify areas of security posture improvement.

Visibility

- SCuBA developed the **extensible Visibility Reference Framework** to enable organizations to identify visibility data, analyze it from a threat-informed perspective, and identify potential visibility gaps.
- WeVRF will provide agencies the ability to build **visibility coverage maps** through an app to easily and consistently identify areas in their architecture where security needs to be bolstered.

Product-Specific Security Baselines

Agency Pilots In Progress

- ✓ Azure Active Directory
- ✓ Defender for Office 365
- ✓ Exchange Online
- ✓ OneDrive for Business
- ✓ Power BI
- ✓ Power Platform
- ✓ SharePoint Online
- ✓ Teams

Targeting Public Comment And Pilot In September 2023

- ✓ Gmail
- ✓ Common Controls
- ✓ Drive/Docs
- ✓ Meet
- ✓ Chat and Classic Hangouts
- ✓ Calendar
- ✓ Groups
- ✓ Sites

Baseline Automation - ScubaGear

- ✓ ScubaGear is an automated tool (PowerShell) that **assesses** an M365 tenant and provides a report on how the configuration measures against the recommended baselines.
- ✓ This tool **reduces the effort** required for agencies to assess themselves and provides a detailed report.
- ✓ ScubaGear was published alongside the baselines to support the pilot effort and is a **driving force for pilot participation.**
- ✓ SCuBA is testing methods that would provide CISA **real-time visibility into tenant configurations** (Multi-Tenant Application Proof of Concept).
- ✓ ScubaGear code updates will be **released on a regular basis** to address Microsoft configuration changes as well as expand automation in development and testing.

Access ScubaGear at: https://github.com/cisagov/scubagear

Microsoft 365 (M365) Baselines Pilot Program

- **CISA** is piloting the M365 baselines with **15 agencies.**
- Pilots began in November 2022
- To date, **11 agencies** have completed their pilot.

*1 - **Reporting Pilot:*** Run the automated assessment tool and share the assessment report with CISA

*2 - **Pilot Feedback:*** Run the assessment tool and review the output & baseline controls with CISA

*3 - **Full Pilot:*** Run the assessment tool, review the controls, and implement controls.

Goals

Improve baselines through **agency feedback** on:

- **Business impact** of controls
- Implementation **blockers** [technical, governance, regulatory]
- **Gaps** in controls

Get feedback on automation for control verification within a tenant (ScubaGear)

Agency Benefits

Increased **security** from recommended settings

CISA **expertise** to understand impact of changes due to controls

Opportunity to **influence** controls

Current and Future Publications

Published

- SCuBA Technical Reference Architecture - June 2023
- Extensible Visibility Reference Framework Guidebook - June 2023

Completed RFC and Nearing Final Publication

- Microsoft 365 Security Configuration Baselines - FY23 Q4
- Hybrid Identity Solutions Architecture - FY24 Q1

Upcoming RFC

- Google Workspace Security Configuration Baselines - FY23 Q4
- Secure Web Gateway Solutions Architecture - FY24 Q1