Cyber Security Controls: Data Portability between vendor tools using NIST OSCAL

J. Travis Howerton
Chief Technology Officer (CTO)
C2 Labs
https://www.c2labs.com
https://atlasity.io
WHO WE ARE
Who We Are

About Us

- **Minority-Owned DC small business:** Founded in 2014, with a diverse workforce & strong nationwide commercial and government past performance

- **Mission:** To serve as a security focused and agile digital transformation partner that blends *Art* and *Science* to enable our customers to expand their vision, drive cultural change, and avoid being left behind

- **Certifications and Awards:** PMP, ITIL, CISSP, DAWIA, AWS, Agile SCRUM Masters, Fed100 Award, ACT-IAC Excellence.gov overall award winner (Most innovative project in Government)

Key Cultural Values

- Innovative
- Driven
- Ethical
- Agile
- Service

“Logic will get you from A to B. Imagination will take you everywhere”

– Albert Einstein
Bio – J. Travis Howerton, C2 Labs Chief Technology Officer

- Travis Howerton is the co-founder and Chief Technology Officer (CTO) of C2 Labs and has previously held positions as the National Nuclear Security Administration CTO, Deputy CIO at Oak Ridge National Laboratory, and the Global Director for Strategic Programs with Bechtel Corporation.

- Howerton holds a B.S. in Organizational Management from Tusculum College, a M.S. in Computer Information Systems from Boston University, and holds multiple certifications to include the CISSP, ITIL, PMP, Scrum Master, Harvard Credential of Readiness, and AWS Certified Developer.

- Howerton is a native of Oak Ridge, TN where he lives with his wife (Beth) and two daughters (Taylor and Sarah Beth).
Abstract

Today, System Security Plans (SSPs) are usually generated in Word or Excel documents using unstructured formats that make them difficult to process in an automated way or to port the information across tools due to the wide variability in formats. In this session, we will discuss how NIST’s OSCAL standard can enable cyber security control data portability, moving cyber security risk and assessment information across different vendor tools using the OSCAL format. By leveraging OSCAL, we will demonstrate:

- The ability to load all OSCAL Catalogs and Baselines of NIST SP 800-53 Rev 4, 5, and FedRAMP Baselines (Low, Moderate, High, and Privacy) into the C2 Labs Atlasity tool
- The ability to load an OSCAL version of an SSP from GovReady (another vendor tool) into Atlasity
- The ability to cross-walk controls from the GovReady SSP against the NIST SP 800-53 FedRAMP Moderate Baseline to load programmatically into Atlasity
- The ability to support leveraged authorizations within Atlasity in support of the OSCAL standard
Hypotheses

This proposal sought to test two hypotheses of the effectiveness of using OSCAL to programmatically load content. These include:

- OSCAL can be used to efficiently load NIST controls to allow the rapid creation of security plans
  - EXAMPLE BENEFIT: Improved quality and time to value by automating the creation of SSPs

- OSCAL can be used to efficiently transfer SSP content programmatically between tools
  - EXAMPLE BENEFIT: Cloud Service Providers could submit SSP content in an automated manner to perform compliance checks with less manual labor and resulting costs (i.e. to FedRAMP)
Experiment 1 – Loading Catalogs and Creating a SSP

Python Script for Loading (271 lines of code)

• C2 Labs downloaded the latest NIST 800-53 and FedRAMP Baselines from the OSCAL GitHub site

• Developed an open-source Python script to parse the OSCAL baseline JSON files, enriched with other data, and bulk uploaded them as catalogs via REST APIs in Atlassian (also published interim artifacts in JSON)

• Developed many Atlasity profiles based on NIST 800-53 Rev. 4, Rev. 5, and FedRAMP

• Used our SSP wizard to create a security plan template in less than 5 minutes after import

• Source code open-sourced @Atlasify

EVIDENCE ON GITHUB: https://github.com/C2-Labs/atlasify/tree/master/oscal

Level of Effort: ~ 15 hours

README: contains detailed process and results info
Experiment 1 – Results

Catalogs Loaded

Profiles Created

SUCCESS
**Experiment 1 – Results**

**SSP Creation**

Welcome to the Security Plan Builder!

This wizard (on boards) will lead you through a standardization plan from templates known as security profiles.

The steps to complete a security plan are as follows:

- Select an applicable security profile from the template. The step will automatically select the correct profile from the profile in the security plan.
- Ensure that any necessary sections are completed and saved for your security plan.

**SSP Visualization**
Experiment 2 – Loading OSCAL SSP from GovReady

Python Script for Loading (662 lines of code)

• The GovReady team provided an example SSP from their tool in OSCAL format for C2 Labs to process
• Developed an open-source Python script to parse the OSCAL SSP JSON file to create the SSP and Control Implementations in Atlasity
• Mapped schema differences between GovReady and Atlasity with OSCAL
• Loaded data programmatically via Atlasity REST APIs
• Source code open-sourced @Atlasify

EVIDENCE ON GITHUB: https://github.com/C2-Labs/atlasify/tree/master/oscal-ssp-import
Level of Effort: ~ 30 hours
README: contains detailed process and results info
Experiment 2 – Results

SSP Loading (Raw Logs)

SSP in Atlasity
Experiment 2 – Results MVP 1

SSP Details

Control Implementation Details
Experiment 2 – Results MVP 2

Components

Parameters
Experiment 2 – Leveraged

Parent Security Plan

Leveraged Authorization
Learnings

- OSCAL standard is extremely robust and can structure huge amounts of content for efficient machine processing
  - Less than 1 week of total programming time to demonstrate these Proof of Concepts with Atlasity and OSCAL

- OSCAL allows for porting data between two separate vendor systems (GovReady and Atlasity)
  - Atlasity can now repeatably import any GovReady SSP via the OSCAL standard using automation

- Atlasity was able to quickly align to OSCAL Release Candidate (RC) nomenclature and constructs to demonstrate feasibility of these use cases providing data on readiness level for other vendors
  - Initial proof point for the broader vendor community

- Demonstrated leveraged authorizations using parent/child security plan relationships (native control inheritance) in Atlasity
  - Important for tiering security plans and for cloud service providers to break out cloud v/s customer responsibilities
Potential Next Steps

- Adding the ability to export SSPs, SAPs, SARs, Catalogs, and Profiles in OSCAL format from Atlasity – using Atlasity Community Edition as a free OSCAL content publishing tool
  - Provides the ability to quickly and easily generate OSCAL content

- Automating Security Assessment Plans (SAPs) and Security Assessment Reports (SARs)
  - Initial integration work has been performed to take automated scan results against DISA STIGS using the MITRE Heimdall tool to automate assessments in Atlasity

- Leveraging the Atlasity Issues module for managing Plans of Actions and Milestones (POAMs)
  - Automating tracking of security deficiencies from automated scanning and CDM tools

- Community feedback and sharing lessons learned with the NIST OSCAL and ATARC teams from this POC for continuous improvement

- Development of PIP or NPM packages for handling OSCAL content
  - Lower barrier of entry for adoption by tool vendors and other developers