Leveraging OSCAL in AWS

Rick Kidder
Sr. Cloud Consultant
11 Jun 2024
Agenda

Discuss the challenges of attaining an ATO
Discuss the Shared Responsibility Model
Discuss the different layers of the Compliance Framework
Discuss how each layer's compliance can be proven, reported
Effectively Communicating Compliance Posture

In order to do this we need to standardize reporting, storytelling, and evidence artifacts

1. Articulating compliance posture across all layers of the compliance framework:

2. Maintaining consistency in reporting, storytelling, and evidence artifacts:

3. Integrating the above elements effectively:
Shared Responsibility Model
Shared Responsibility

Cloud Resources /Services

Cloud Brokerage (SCCA)

OS, Applications, Networking

CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTTEGRITY, IDENTITY)

P-ATO

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS
Leveraging Security Hub & Config

Security Hub and its NIST SP 800-53 Operational Best Practices (OPB) and AWS Config NIST SP 800-53 OPB Conformance Packs both provide a mechanism to assess the recommended configuration of cloud resources and services.
Security Hub Compliance Analyzer

Security Hub and its NIST SP 800-53 Operational Best Practices (OPB) and AWS Config NIST SP 800-53 OPB Conformance Packs both provide a mechanism to assess the recommended configuration of cloud resources and services.
SHCA and Security Hub Output

Security Hub Finding

This output would represent individual findings of the assessments performed by Security Hub for each unique resource or service assessed by a unique Security Hub Rule.

NIST SP 800-53 Control

This output would represent a compliance percentage at the top level control by calculating the results of all Security Hub rules related to a unique control against all applicable resources.
References


https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format-syntax.html

https://github.com/awslabs/security-hub-compliance-analyzer
Questions?