CI Test Results Report Format
Version 0.8

Amit Kapoor

05-31-2024

Contents

© 2024 SCMS Manager LLC, All Rights Reserved.

1 Abstract

This report, as part of the Utah Smartgrant initiative, outlines a recommended format for traffic organizations to use when providing cybersecurity test results for connected intersections to Security Credential Management System (SCMS) providers. This machine-readable format is crucial for maintaining accurate and up-to-date cybersecurity information throughout the lifecycle of the connected intersection. By adopting this standardized format, SCMS providers can automate the certification process, ensuring continuous compliance and security monitoring, and enhancing the overall efficiency and effectiveness of the cybersecurity management for connected intersections.

2 Status of This Standard

This is a standard being proposed by SCMS Manager for all IOOs and SCMS providers under the Utah Smart Grant project.

© 2024 SCMS Manager LLC, All Rights Reserved.

3 Introduction

The integration of Secure Credential Management System (SCMS) in connected intersections is critical to ensuring secure and reliable communication within the Vehicle-to-Everything (V2X) ecosystem. SCMS providers play a crucial role in issuing and managing digital certificates that authenticate V2X messages, ensuring the integrity, authenticity, and confidentiality of data exchanges between vehicles, infrastructure, and other entities. These certificates are essential for building trust in the V2X network, preventing malicious actors from injecting false data, and maintaining the overall safety and efficiency of traffic systems. Certificates are issued to various components and parties in the ecosystem, such as vehicles, roadside units, and infrastructure elements, ensuring that each entity in the network can be reliably authenticated.

To maintain a high level of security and operational efficiency, SCMS providers require detailed technical reports from each connected intersection reflecting implementation of various cybersecurity controls. These reports must confirm that intersections are functioning correctly, adhering to mandated security protocols, and capable of securely managing the digital certificates issued by the SCMS provider. The reports will enable SCMS providers to issue initial certificates and continue renewing them, ensuring that only compliant and secure intersections remain part of the V2X network. For streamlined processing and integration into existing systems, these reports must be in a machine-readable format, allowing for automated analysis and quick decision-making.

© 2024 SCMS Manager LLC, All Rights Reserved.

3.1 Terminology

- **V2X (Vehicle-to-Everything)**: A communication technology that enables vehicles to interact with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and networks (V2N) to enhance traffic safety, efficiency, and convenience.
- **SCMS (Secure Credential Management System)**: A system that manages digital certificates used to authenticate V2X messages, ensuring the integrity, authenticity, and confidentiality of communications within the V2X ecosystem.
- **Digital Certificates**: Electronic documents used to verify the identity of entities (vehicles, infrastructure) within the V2X network. Issued by the SCMS, these certificates ensure secure communication by providing cryptographic proof of identity.
- **Cryptographic Keys**: Secure digital codes used in cryptographic algorithms to encrypt and decrypt data, ensuring the confidentiality and integrity of communications within the V2X system.
- **JSON (JavaScript Object Notation)**: A lightweight, text-based data interchange format that is easy for humans to read and write and easy for machines to parse and generate. Commonly used for transmitting data in web applications.
- **XML (eXtensible Markup Language)**: A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Often used in enterprise systems for data interchange.
- **Protobuf (Protocol Buffers)**: A method developed by Google for serializing structured data, more efficient in terms of performance and space compared to JSON and XML. Used for transmitting data across network services.
- **Latency**: The time taken for a message to travel from its source to its destination in a network. Low latency is crucial for real-time V2X communications to ensure timely and accurate information exchange.
- **Throughput**: The amount of data successfully transmitted from one place to another in a given amount of time. High throughput is essential for handling the large volume of data in V2X communications.
- **Certificate Revocation**: The process of invalidating a previously issued digital certificate before its scheduled expiration date. This is done if the certificate is compromised or no longer trusted.
- **Key Management**: The process of handling cryptographic keys, including their generation, exchange, storage, use, and replacement. Proper key management is vital for maintaining the security of V2X communications.
- **Interference**: Disruptions in communication signals caused by external factors such as physical obstacles, other electronic devices, or environmental conditions. Minimizing interference is essential for reliable V2X communications.
- **Anomaly Detection**: The process of identifying unusual patterns or behaviors in data that do not conform to expected norms. In V2X systems, anomaly detection helps in identifying potential security breaches or operational issues.
- **Machine-Readable Format**: Data formats that are easily processed by computers, enabling automated systems to read, interpret, and act on the data without human intervention. Common formats include JSON, XML, and Protobuf.
- **Encryption Protocols**: Algorithms and standards used to encrypt data, ensuring its confidentiality and integrity during transmission. Common protocols include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- **Incident Response**: The actions taken by an organization to address and manage the aftermath of a security breach or cyberattack. Effective incident response is critical for minimizing damage and restoring normal operations in V2X systems.

© 2024 SCMS Manager LLC, All Rights Reserved.

- OSCAL (Open Security Controls Assessment Language): A set of standardized, machine-readable formats (XML, JSON, YAML) developed by NIST to enhance the efficiency and consistency of security control assessments.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in (Bradner 1997).

© 2024 SCMS Manager LLC, All Rights Reserved.

4 Report Requirements

1. **Operational Status**
   - *Health Check*: Includes information about the intersection's operational status, such as uptime, system diagnostics, and any detected anomalies.
   - *Sensor and Device Status*: Details the status of all connected sensors and devices, including their operational state, firmware versions, and any fault reports.
   - *Data Integrity Checks*: Ensures the data being transmitted by the intersection's systems is accurate and untampered.
   - *Message Logs*: Logs of V2X messages sent and received, including timestamps, message types, and any errors encountered.
   - *Latency and Throughput Metrics*: Performance metrics for message transmission, including average and peak latency, and data throughput.
   - *Interference Reports*: Reports on any detected interference or disruptions in communication channels.
2. **Security Compliance**
   - *Certificate Status*: Provides details on the current status of all certificates used by the intersection, including expiration dates and any revocations.
   - *Key Management*: Information on key generation, storage, and usage policies, including audit logs of key usage.
   - *Incident Reports*: Logs of any security incidents, such as attempted breaches, detected intrusions, and responses to these incidents.
   - *Encryption Protocols*: Details on the encryption standards and protocols in use, including any updates or changes made.

4.1 Machine-Readable Format

To ensure that these reports can be automatically processed by SCMS providers, they must be delivered in a machine-readable format. This can be achieved through standardized data formats such as JSON, XML, YAML, or Protocol Buffers (Protobuf). The choice of format will depend on the specific requirements of the SCMS provider and the existing infrastructure of the connected intersections. However, in this report, there will be a recommndation for a canonical format.

- **JSON (JavaScript Object Notation)**: A lightweight data-interchange format that is easy to read and write for humans and machines. Ideal for systems with a preference for web-based technologies.
- **XML (eXtensible Markup Language)**: A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Commonly used in enterprise applications.
- **Protocol Buffers (Protobuf)**: A method developed by Google for serializing structured data, more efficient in terms of performance and space compared to JSON and XML.
- **YAML (YAML Ain't Markup Language)**: YAML is a human-readable data serialization standard that is commonly used for configuration files and data exchange between languages with different data structures. It is designed to be simple and easy to read, making it ideal for developers and system administrators.

© 2024 SCMS Manager LLC, All Rights Reserved.

5 Implementation Strategy

- **Report Schemas**: Develop comprehensive report format ensuring all necessary information is included and correctly formatted.
- **Automated Report Generation**: Implement systems at each intersection that can automatically generate the required reports at specified intervals or upon specific triggers.
- **Secure Transmission**: Ensure the secure transmission of reports from intersections to the SCMS provider, using encryption protocols to protect the data in transit.
- **Validation and Auditing**: Develop mechanisms for the SCMS provider to validate the received reports, checking for completeness, accuracy, and compliance with security standards.
- **Feedback Loop**: Establish a feedback loop where the SCMS provider can notify intersections of any issues detected in the reports, prompting corrective actions.
- **CI Lifecycle**: Supporting a Connected Intersection (CI) through its full lifecycle for security certification involves continuous monitoring, regular assessments, and periodic updates to ensure compliance with security standards, the effectiveness of implemented controls, and the issuance and management of necessary digital certificates to maintain secure operations.

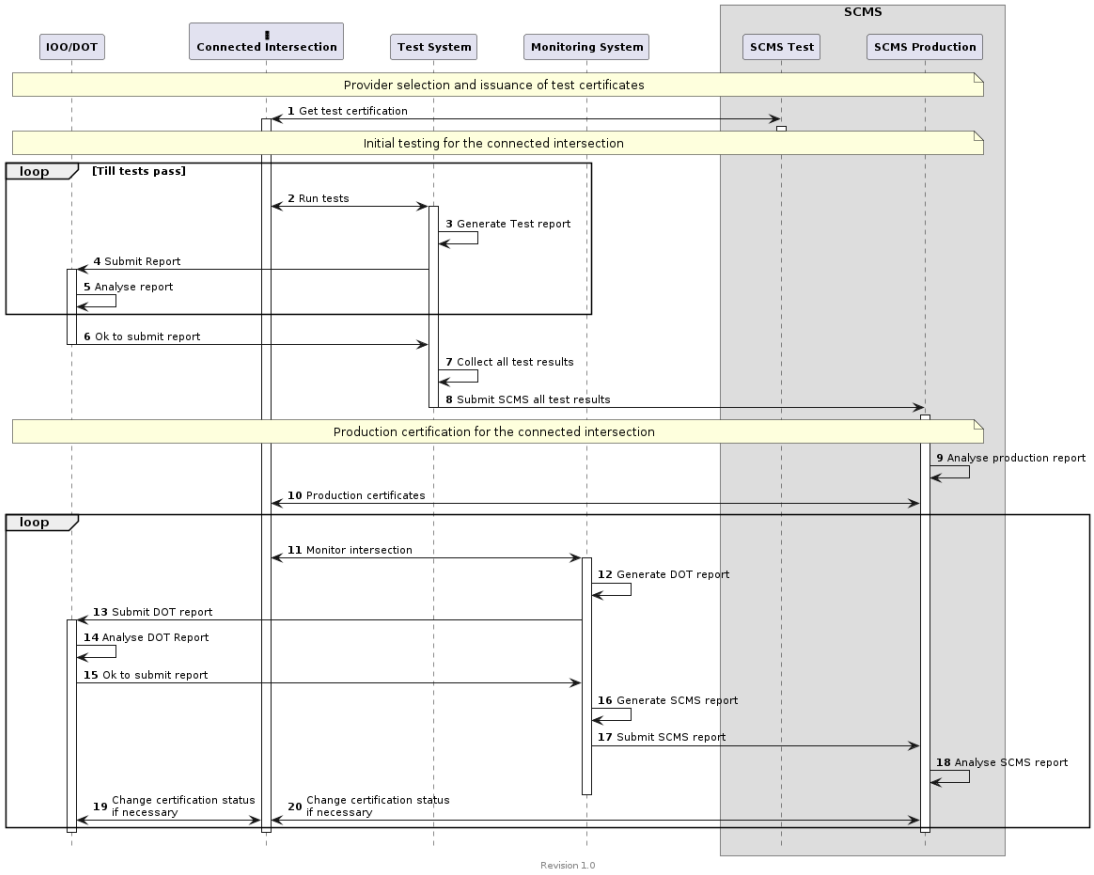

Figure 1: Report Flows

When implementing a cybersecurity assessment report for connected intersections, it is highly recommended to adopt an already established format rather than designing a new custom one. Using a pre-existing format offers several advantages:

- **Standardization**: Leveraging a widely recognized format ensures consistency and compatibility across various systems and organizations.

© 2024 SCMS Manager LLC, All Rights Reserved.

- **Interoperability**: Existing formats are designed to work seamlessly with different tools and platforms, facilitating smoother integration and data exchange.
- **Proven Reliability**: Established formats have undergone extensive testing and validation, minimizing the risk of errors and issues.
- **Efficiency**: Implementing a pre-existing format reduces development time and effort, allowing organizations to focus on other critical aspects of the cybersecurity assessment process.

By choosing a well-supported and widely accepted format, organizations can ensure robust, efficient, and secure reporting mechanisms that align with industry best practices.

© 2024 SCMS Manager LLC, All Rights Reserved.

6 Introduction to OSCAL

6.1 What is OSCAL?

The Open Security Controls Assessment Language **(OSCAL)** is a set of hierarchical, structured formats expressed in XML, JSON, and YAML. Developed by the **National Institute of Standards and Technology (NIST)**, OSCAL standardizes the representation of information in information security, particularly for security controls, assessments, and continuous monitoring. The goal is to facilitate automation, improve efficiency, and ensure consistency in managing security controls across various frameworks and organizations.

6.2 Key Objectives

6.2.1 Standardization

OSCAL provides a common language for expressing security controls, assessments, and related information, reducing complexity and improving interoperability between different systems and tools.

6.2.2 Automation

With **machine-readable formats**, OSCAL supports the automation of security assessment processes, significantly reducing the time and effort required for compliance checks, risk assessments, and continuous monitoring.

6.2.3 Consistency

Using OSCAL ensures that security control information is consistent across different frameworks and organizations, which is crucial for effective risk management and meeting regulatory requirements.

6.3 OSCAL Layers and Models

OSCAL is organized into three main layers, each consisting of one or more models that address specific aspects of security controls and assessments.

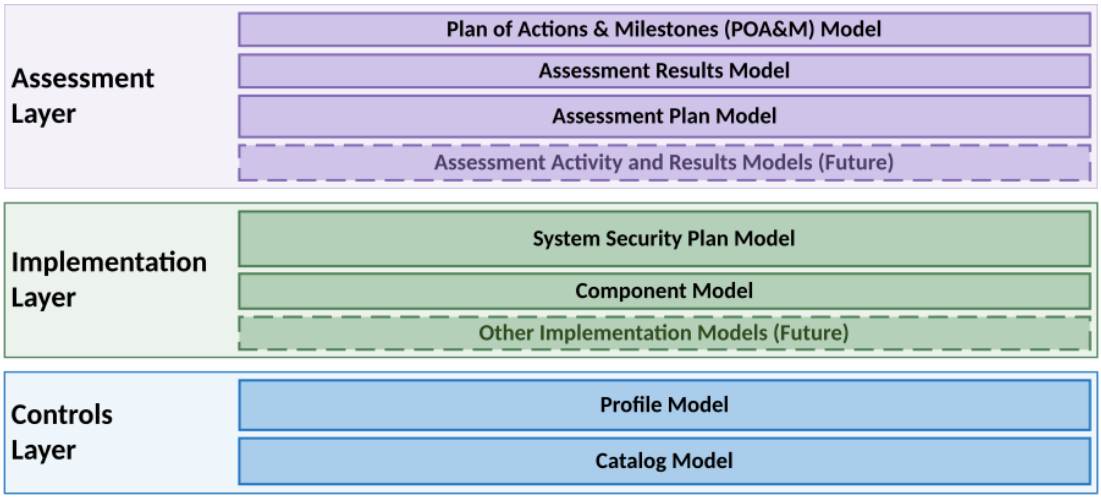

Figure 2: OSCAL Layers

6.3.1 Control Layer

The Control Layer focuses on the representation and organization of security controls. It includes:

- **Catalog Model:** Organizes security controls into a catalog, supporting various frameworks.

© 2024 SCMS Manager LLC, All Rights Reserved.

- **Profile Model:** Enables the selection and tailoring of controls to create a specific set, known as a profile.

6.3.2 Implementation Layer

The Implementation Layer addresses how security controls are implemented within a system. It includes:

- **System Security Plan (SSP) Model:** Describes how security controls are implemented within an information system.
- **Component Definition Model:** Defines individual components that can satisfy controls, such as policies, processes, hardware, software, or services.

6.3.3 Assessment Layer

The Assessment Layer focuses on assessing the implementation and effectiveness of security controls. It includes:

- **Assessment Plan Model:** Outlines the plan for conducting security assessments.
- **Assessment Results Model:** Captures the results of security assessments, including findings, evidence, and observations.
- **Plan of Action and Milestones (POA&M) Model:** Tracks the remediation of identified issues.

6.4 Benefits of OSCAL

6.4.1 Improved Efficiency

Standardizing and automating security control assessments significantly reduces the time and effort required for compliance and risk management activities.

6.4.2 Enhanced Interoperability

OSCAL's machine-readable formats facilitate the exchange of information between different systems and tools, improving interoperability and reducing the risk of errors.

6.4.3 Better Risk Management

Consistent and accurate representation of security controls helps organizations manage risks more effectively, ensuring compliance with regulatory requirements and protection of their information systems.

6.4.4 Scalability

OSCAL's structured formats and support for automation make it easier to scale security assessments and continuous monitoring across large and complex environments.

6.5 Summary

OSCAL represents a significant advancement in the standardization and automation of security controls assessment and management. By adopting OSCAL, organizations can improve the efficiency, consistency, and effectiveness of their security programs, enhancing their ability to manage risks and comply with regulatory requirements. As OSCAL continues to evolve, it is poised to play a critical role in the future of cybersecurity management.

For more detailed information and updates on OSCAL, visit the NIST OSCAL website.

© 2024 SCMS Manager LLC, All Rights Reserved.

7 OSCAL Assessment Report Format

The OSCAL Assessment Results model defines the information contained within an assessment report supporting assessment and continuous monitoring capabilities. The OSCAL Assessment Results model is part of the OSCAL Assessment Layer. It defines structured, machine-readable XML, JSON, and YAML representations of the information contained within an assessment report.

This model is typically used by anyone performing assessment or continuous monitoring activities on a system to determine the degree to which that system complies with one or more frameworks.

This model allows an assessor to express all details associated with a classic "snapshot in time" assessment, including the scope of the assessment, times and dates of activities, actual assessment activities performed, as well as any observations, findings, and identified risks. It also allows organizations to report continuous assessment information.

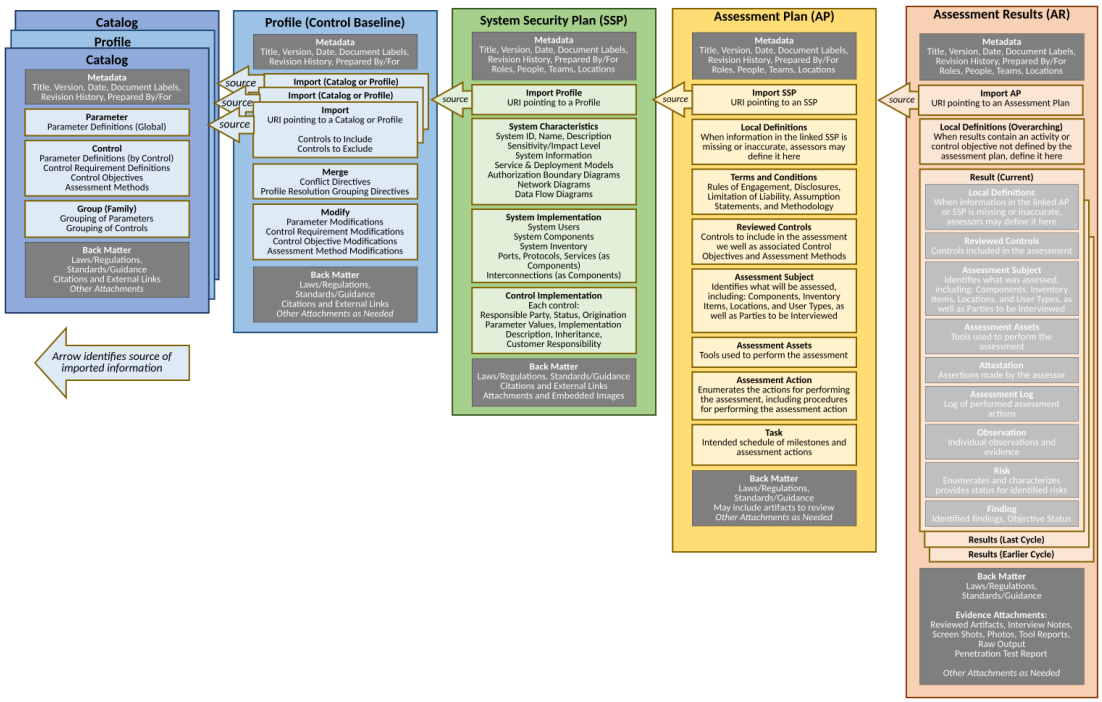

Figure 3: OSCAL Assesment Report

7.1 Assessment Results Organization

An OSCAL assessment report is organized as follows:

- **Metadata**: Metadata syntax is identical and required in all OSCAL models. It includes information such as the file's title, publication version, publication date, and OSCAL version. Metadata is also used to define roles, parties (people, teams and organizations), and locations.
- **Import AP**: Identifies the OSCAL-based assessment plan (AP) for this assessment. The AP imports several pieces of information about the system being assessed including the system security plan (SSP), which is also represented according to the OSCAL SSP model. This linking of data eliminates the need to duplicate and maintain the same information in multiple places.
- **Local Definitions**: When the assessment results contain an activity or control objective not defined by the assessment plan, assessors define it here instead.
- **Results**: Describes the assessment findings, identified risks, and recommended remediation. Also identifies false positive results, risk adjustments, and operationally required risks, as well as when the results should expire.

© 2024 SCMS Manager LLC, All Rights Reserved.

  - Local Definitions: Normally other aspects of the assessment results point to content in the linked Assessment Plan and SSP. When the AR must reference information that is missing from the linked AP or SSP, assessors define it here instead.
  - Reviewed Controls: Identifies the controls actually reviewed by this assessment.
  - Assessment Subject: Identifies the in-scope elements of the system, including locations, components, inventory items, and users.
  - Assessment Assets: Identifies the assessor's assets used to perform the assessment, including the team, tool, and rules of engagement content.
  - Attestation: Assertions made by the assessor.
  - Assessment Log: Log of performed assessment actions. This includes start and end timestamps for individual actions performed by the assessment team, with an optional link to defined assessment actions.
  - Observation: Individual observations and related evidence. This may be evidence of compliance or non-compliance.
  - Risk: Identifies individual risks, including weakness description, risk statement, and other risk characteristics.
  - Finding: Identifies findings resulting from observations and risks, and can include the control objective status.
- **Back Matter**: Back matter syntax is identical in all OSCAL models. It is used for attachments, citations, and embedded content such as graphics.

7.2 OSCAL Assessment Report Example


```
{
  "assessment-results": {
    "uuid": "ec0dad37-54e0-40fd-a925-6d0bdea94c0d",
    "metadata": {
    "title": "IFA GoodRead Continuous Monitoring Assessment Results June 2023",
      "last-modified": "2024-02-01T13:57:28.355446-04:00",
      "version": "202306-002",
      "oscal-version": "1.1.2",
      "roles": [
        {
          "id": "assessor",
          "title": "IFA Security Controls Assessor"
        }
      ],
      "parties": [
        {
          "uuid": "e7730080-71ce-4b20-bec4-84f33136fd58",
          "type": "person",
          "name": "Amy Assessor",
          "member-of-organizations": [
            "3a675986-b4ff-4030-b178-e953c2e55d64"
          ]
        },
        {
          "uuid": "3a675986-b4ff-4030-b178-e953c2e55d64",
          "type": "organization",
          "name": "Important Federal Agency",
          "short-name": "IFA",
          "links": [
            {
              "href": "https://www.ifa.gov",
              "rel": "website"
```


© 2024 SCMS Manager LLC, All Rights Reserved.

```
        }
      ]
    }
  ],
  "responsible-parties": [
    {
      "role-id": "assessor",
      "party-uuids": [
        "e7730080-71ce-4b20-bec4-84f33136fd58"
      ]
    }
  ]
},
"import-ap": {
  "href": "./ap.oscal.xml"
},
"local-definitions": {
  "activities": [
    {
      "uuid": "cf5d53fe-6043-4c68-9ed6-6b258909febf",
      "title": "Test System Elements for Least Privilege Design and
      Implementation",
     "description": "The activity and it steps will be performed by the
      assessor via their security automation platform to test least
      privilege design and implementation of the system's elements,
    specifically the cloud account infrastructure, as part of continuous
      monitoring.",
      "props": [
        {
          "name": "method",
          "value": "TEST"
        }
      ],
      "steps": [
        {
          "uuid": "57f8cfb8-fc3f-41d3-b938-6ab421c92574",
        "title": "Configure Cross-Account IAM Role Trust for GoodRead and
          Assessor AwesomeCloud Accounts",
        "description": "The GoodRead system engineer will coordinate with
        the assessor's engineering support staff to configure an IAM role
          trust. A service account for automation with its own role with
          the assessor's AwesomeCloud account can assume the role for
         read-only assessor operations within the GoodRead Product Team's
          AwesomeCloud account for continuous monitoring of least
          privilege.",
         "remarks": "This step is complete.\n\nGoodRead Product Team and
          SCA Engineering Support configured the latter's cross-account
          role trust and authentication and authorization in to the
          former's account on May 29, 2023."
        },
        {
          "uuid": "976aadad-b1ce-475b-aa6c-e082537e7902",
     "title": "Automate Cross-Account Login to GoodRead AwesomeCloud Account",
        "description": "The assessor's security automation platform will
         create a session from their dedicated will obtain access to the
```

© 2024 SCMS Manager LLC, All Rights Reserved.

```
          GoodRead Product Team's AwesomeCloud account with their single
           sign-on credentials to a read-only assessor role.",
          "remarks": "This step is complete.\n\nGoodRead Product Team and
           SCA Engineering Support tested scripts from the security
           automation platform interactively on May 30, 2023, to confirm
           they work ahead of June 2023 continuous monitoring cycle."
         },
         {
           "uuid": "18ce4e19-7432-4484-8e75-2dd8f05668cf",
          "title": "Analyze GoodRead Developer and System Engineer Roles
           for Least Privilege",
           "description": "Once authenticated and authorized with a
           cross-account session, the security automation pipeline will
           execute scripts developed and maintained by the assessor's
         engineering support staff. It will analyze the permitted actions
           for the developer and system engineer roles in the GoodRead
         Product Team's AwesomeCloud account to confirm they are designed
           and implement to facilitate only least privilege operation.
        Examples are included below.\n\n* For the GoodRead developer role
        in their AwesomeCloud account, the developer role may only permit
         the user with this role to check the IP addresses and status of
        the Awesome Compute Service server instances. This role will not
           permit the user to create, change, or delete the instances.
        Similarly, the developer will permit a user to perform actions to
          see IP addresses of an Awesome Load Balancer instance, but not
        add, change, or delete the instances.\n* For the GoodRead system
        engineer role in their AwesomeCloud account, the system engineer
         role may only permit actions where the user can add, change, or
           delete instances for approved services (i.e. Awesome Compute
            Service, Awesome Load Balancer, et cetera). The role may not
             permit actions by the user for any other service.\n"
         }
       ],
       "related-controls": {
         "control-selections": [
           {
             "include-controls": [
               {
                 "control-id": "ac-6.1"
               }
             ]
           }
         ]
       },
       "responsible-roles": [
         {
           "role-id": "assessor",
           "party-uuids": [
             "e7730080-71ce-4b20-bec4-84f33136fd58"
           ]
         }
       ]
     }
   ]
 },
```


© 2024 SCMS Manager LLC, All Rights Reserved.

```
"results": [
  {
    "uuid": "a1d20136-37e0-42aa-9834-4e9d8c36d798",
    "title": "IFA GoodRead Continous Monitoring Results June 2023",
  "description": "Automated monthly continuous monitoring of the GoodRead
   information system's cloud infrastructure recorded observations below.
   Additionally, contingent upon the confidence level of the observations
    and possible risks, confirmed findings may be opened.",
    "start": "2023-06-02T08:31:20-04:00",
    "end": "2023-06-02T08:46:51-04:00",
    "local-definitions": {
      "tasks": [
        {
          "uuid": "35876484-aa4b-494d-95a2-0d1cc04eb47e",
          "type": "action",
          "title": "Test System Elements for Least Privilege Design and
          Implementation",
         "description": "The activity and it steps will be performed by
       the assessor via their security automation platform to test least
          privilege design and implementation of the system's elements,
          specifically the cloud account infrastructure, as part of
          continuous monitoring.",
          "associated-activities": [
            {
              "activity-uuid": "cf5d53fe-6043-4c68-9ed6-6b258909febf",
              "subjects": [
                {
                  "type": "component",
                  "include-all": {}
                }
              ]
            }
          ]
        }
      ]
    },
    "reviewed-controls": {
      "control-selections": [
        {
          "include-controls": [
            {
              "control-id": "ac-6.1"
            }
          ]
        }
      ]
    },
    "observations": [
      {
        "uuid": "8807eb6e-0c05-43bc-8438-799739615e34",
    "title": "AwesomeCloud IAM Roles Test - GoodRead System Engineer Role",
        "description": "Test AwesomeCloud IAM Roles for least privilege
        design and implementation.",
        "methods": [
          "TEST"
```


© 2024 SCMS Manager LLC, All Rights Reserved.

```
      ],
      "types": [
        "finding"
      ],
      "subjects": [
        {
          "subject-uuid": "551b9706-d6a4-4d25-8207-f2ccec548b89",
          "type": "component"
        }
      ],
      "collected": "2023-06-02T08:31:20-04:00",
      "expires": "2023-07-01T00:00:00-04:00",
     "remarks": "The assessor's security automation platform analyzed
    all roles specific to the GoodRead Product Team, not those managed
      by the Office of Information Technology. The
    `IFA-GoodRead-SystemEnginer` role in their respective AwesomeCloud
      account permitted use of the following high-risk actions.\n\n*
      awesomecloud:auditlog:DeleteAccountAuditLog\n*
      awesomecloud:secmon:AdministerConfigurations\n\n\nBoth of these
    actions are overly permissive and not appropriate for the business
      function of the staff member assigned this role."
    },
    {
      "uuid": "4a2fb32e-9be9-43cf-b717-e9e47de061bd",
     "title": "AwesomeCloud IAM Roles Test - GoodRead Developer Role",
      "description": "Test AwesomeCloud IAM Roles for least privilege
      design and implementation.",
      "methods": [
        "TEST"
      ],
      "types": [
        "finding"
      ],
      "subjects": [
        {
          "subject-uuid": "551b9706-d6a4-4d25-8207-f2ccec548b89",
          "type": "component"
        }
      ],
      "collected": "2023-06-02T08:31:20-04:00",
      "expires": "2023-07-01T00:00:00-04:00",
     "remarks": "The assessor's security automation platform detected
    that the developer's role is permitted to perform only permissible
    actions in the GoodRead AwesomeCloud account in accordance with the
      agency's least privilege policy and procedures."
    }
  ],
  "risks": [
    {
      "uuid": "0cfa750e-3553-47ba-a7ba-cf84a884d261",
  "title": "GoodRead System Engineers Have Over-Privileged Access to Cloud Infrastructur
     "description": "A user in the GoodRead cloud environment with the
    privileges of a system engineer can exceed the intended privileges
    for their related business function. They can delete all historical
      audit records and remove important security monitoring functions
```


© 2024 SCMS Manager LLC, All Rights Reserved.

```
            for the IFA Security Operations Center staff.",
          "statement": "An account without proper least privilege design and
            implementation can be used to surreptitiously add, change, or
           delete cloud infrastructure to the too managing all links to IFA's
           communication to public citizens, potentially causing significant
          harm with no forensic evidence to recover the system. Regardless of
            the extent and duration of a potential incident, such a
           configuration greatly increases the risk of an insider threat if
            there were likely to a potential insider threat in the GoodRead
           Product Team.\n\nIf such an insider threat existed and acted with
           this misconfigruatio, the resulting event could cause significant
           financial and reputational risk to IFA's Administrator, executive
            staff, and the agency overall.",
            "status": "investigating"
          }
        ],
        "findings": [
          {
            "uuid": "45d8a6c2-1368-4bad-9ba0-7141f0a32889",
            "title": "GoodRead AwesomeCloud Account's System Engineer Role
            Permits High Risk Actions",
            "description": "The assessor's security automation platform
           detected that the system engineer's role is permitted to perform
           the following actions in the GoodRead AwesomeCloud account.\n\n*
            Delete and reset account audit logs.\n* Add, change, or delete
           security monitoring configurations in the Awesome Security Monitor
          service used by the IFA Security Operations Center.\n\n\nThe system
           engineer is not permitted to modify these services and their role
            was incorrectly configured.",
            "target": {
              "type": "objective-id",
              "target-id": "ac-6.1_obj",
              "description": "This is a finding.",
              "status": {
                "state": "not-satisfied"
              }
            },
        "implementation-statement-uuid": "d5f9b263-965d-440b-99e7-77f5df670a11",
            "related-observations": [
              {
                "observation-uuid": "8807eb6e-0c05-43bc-8438-799739615e34"
              }
            ],
            "related-risks": [
              {
                "risk-uuid": "0cfa750e-3553-47ba-a7ba-cf84a884d261"
              }
            ]
          }
        ]
      }
    ]
  }
}
```


© 2024 SCMS Manager LLC, All Rights Reserved.

8 Summary

8.1 Standardization and Interoperability

The OSCAL (Open Security Controls Assessment Language) assessment report format provides a standardized, machine-readable way to convey cybersecurity assessment results. By adhering to a common structure and format, organizations can ensure consistency in how security information is reported, making it easier to compare and integrate data across different systems and frameworks. This standardization promotes interoperability, allowing various tools and systems to seamlessly exchange and process security assessment data.

8.2 Automation and Efficiency

One of the key advantages of using the OSCAL assessment report format is the ability to automate the generation, validation, and processing of security assessment reports. Automation reduces the manual effort required to compile and analyze assessment data, thus increasing efficiency and accuracy. With OSCAL, organizations can leverage automated tools to streamline the assessment process, quickly identify compliance gaps, and generate comprehensive reports without the risk of human error.

8.3 Enhanced Risk Management

The OSCAL assessment report format supports detailed and structured documentation of security controls and their assessment results. This structured approach helps organizations maintain a clear and comprehensive view of their security posture, facilitating better risk management. By providing a transparent and consistent way to report on security controls, OSCAL enables organizations to more effectively monitor and manage risks, ensuring that security measures are adequately implemented and maintained.

8.4 Facilitating Continuous Monitoring

In the rapidly evolving cybersecurity landscape, continuous monitoring is crucial for maintaining a robust security posture. The OSCAL assessment report format supports ongoing assessment and monitoring activities by providing a consistent and repeatable method for documenting and reporting security control assessments. This capability allows organizations to maintain up-to-date security information, quickly respond to emerging threats, and ensure continuous compliance with regulatory requirements.

8.5 Conclusion

The OSCAL assessment report format offers significant benefits in terms of standardization, automation, risk management, and continuous monitoring. By adopting OSCAL, organizations can improve the efficiency and effectiveness of their cybersecurity assessments, ensuring that they can quickly adapt to changing security landscapes and maintain robust protection for their information systems.

© 2024 SCMS Manager LLC, All Rights Reserved.

Bibliography

Bradner, Scott. 1997. “Key Words for Use in Rfcs to Indicate Requirement Levels.” BCP 14. RFC Editor; Internet Requests for Comments; RFC Editor. http://www.rfc-editor.org/rfc/rfc2119.txt.

© 2024 SCMS Manager LLC, All Rights Reserved.