Initial Experiences with OSCAL and Continuous Monitoring in the EUCS

Dr. Jesus Luna Garcia
Robert Bosch GmbH, Germany
Agenda

- Background
- Experimenting with EUCS-Continuous & OSCAL
- Summary
Background

EU Cybersecurity Act (EUCSA)
EU Cybersecurity Certification Scheme for Cloud Services (EUCS)
The EU Cybersecurity Act (EUCSA, April 2019), proposes the creation EU-wide cybersecurity certification schemes in order to:

- provide an EU-wide cybersecurity baseline (requirements, audit methods)
- enable customers to make risk-based decisions about cybersecurity
- enable **continuous cybersecurity compliance**

Two EUCSA-derived certification schemes are under preparation by ENISA:

- EUCC – Cybersecurity Certification Scheme for Common Criteria
- **EUCS - Cybersecurity Certification Scheme for Cloud Services**
EUCS at a glance – Scope on Cloud Services

Customers / Consumers

BOSCH

Smart Home Product 1
Smart Home Services 1
Smart Home Product n
Smart Home Services n

uses / integrates

Hyperscaler

BOSCH

Smart Home Azure Service
Customer Identity & Access Management (CIAM)
VM Kubernetes SQL Blockchain Storage Serverless Etc.

Cloud Platform
EUCS at a glance – Scope on Cloud Services

BOSCH

Smart Home Product 1
Smart Home Services 1
Smart Home Product n
Smart Home Services n

Customers / Consumers

buys / uses

buys / uses

buys / uses

buys / uses

EUCC, EUIoT, EUAI

uses / integrates

EUSG

Hyperscaler

BOSCH

Smart Home Azure Service
Customer Identity & Access Management (CIAM)
VM Kubernetes SQL Blockchain Storage Serverless Etc

Cloud Platform

EUCS
Defining Continuous Monitoring in EUCS

Continuous monitoring

The requirements related to continuous monitoring typically mention "automated monitoring" or "automatically monitor" in their text. The intended meaning of "monitor automatically" is:

1. Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;
2. Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;
3. Report deviations to subject matter experts who can analyse the deviations in a timely manner;
4. If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and
5. If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.

These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity. Nevertheless, the introduction of continuous auditing, at least for level High, remains a mid- or long-term objective, and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.

Further guidance will be provided about acceptable mechanisms and processes.

Source: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
Defining Continuous Monitoring in EUCS

Just “gather, compare, & report”

WHAT COULD POSSIBLY GO WRONG?

Source: https://starecat.com/what-could-possibly-go-wrong-cutting-fail/
Experimenting with EUCS-Continuous and OSCAL

H2020 MEDINA Project
Why the EU-funded MEDINA Project?

Let’s understand the real-world implications from an EUCS perspective...

...and one day we will fully realize automation in EUCS processes!
MEDINA At a Glance

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€
**Paving to Road for EUCS-Continuous**

<table>
<thead>
<tr>
<th>Existing Certifications</th>
<th>Approach in MEDINA</th>
</tr>
</thead>
</table>
| Assurance based on point-in-time assessments                 | Continuous audit-based certification  
 Tamper-proof evidence stored in DLT                                                |
| Mostly manual/time consuming assessment processes            | NLP to ease assessment of organizational measures  
 OSCAL automation for CSP-agnostic assessments                         |
| Lack of transparency in cloud security posture               | Role-based visualizations provide different levels of granularity and assurance for EUCS certificates |
| High customization effort in commercial CSPM tools (Cloud Security Posture Management) | Automated generation of compliance assessment rules based derived from EUCS catalogue |
Experimenting with EUCS

In March 2021, ENISA released a “call for experimentation” related to different aspects of the candidate EUCS.

MEDINA contributed with the experimentation of automated monitoring requirements, including an OSCAL – EUCS PoC.

- Running period: 30 days
- Testbed: well-known hyperscaler
- Tools: hyperscaler’s CSPM, MEDINA’s homebrew metrics & dashboards
Obtained Results

- OSCAL format for EUCS:
  - Machine-readability benefits EUCS automation
  - NIST OSCAL as a promising alternative for representing EUCS catalogue and assessments

<table>
<thead>
<tr>
<th>OSCAL</th>
<th>EUCS</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups/ID</td>
<td>Domain</td>
<td>A7</td>
</tr>
<tr>
<td>Groups/title</td>
<td>Category</td>
<td>A7 Operational Security</td>
</tr>
<tr>
<td>Groups/parts/prose(objective)</td>
<td>Objective</td>
<td>Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures</td>
</tr>
<tr>
<td>Groups/Controls/properties/value(label)</td>
<td>Control ID</td>
<td>OPS-02</td>
</tr>
<tr>
<td>Groups/Controls/title</td>
<td>Control</td>
<td>CAPACITY MANAGEMENT - MONITORING</td>
</tr>
<tr>
<td>Groups/Controls/parts/prose/(control-objective)</td>
<td>Control Objective</td>
<td>The capacities of critical resources such as personnel and IT resources are monitored.</td>
</tr>
<tr>
<td>Groups/Controls/parts/parts/properties/value(label)</td>
<td>Requirement ID</td>
<td>OPS-02.3</td>
</tr>
<tr>
<td>Groups/Controls/parts/parts/prose(item)</td>
<td>Requirement</td>
<td>The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1</td>
</tr>
</tbody>
</table>
Let’s not Forget About the Auditors’ Perspective!

- The experiment shown that (very) different levels of automation can be achieved for implemented EUCS requirements.
- Auditor’s involvement is still required to ensure that the automated monitoring provides trustworthy evidence.
- Standardization of audit processes, good practices (including EUCS Metrics) is still needed to leverage the full potential of automation.

About the auditor’s toolset:
  - Egg-chicken problem – who certifies the tools for certification?
Summary

What comes next?
How-To EUCS-Continuous?

1. Provide a clear **implementation guidance** about EUCS requirements where some degree of automated monitoring is needed.

2. Provide clear **audit/assessment guidance** related to EUCS requirements needing some degree of automated monitoring.

3. Consider integrating a **catalogue of metrics** as part of the implementation guidance for EUCS.

4. Consider **focusing the EUCS requirements** needing some sort of automated monitoring only on capabilities offered by cloud platforms, and not by external systems.

5. **Guidance on selecting tools/technologies** for automated (continuous) monitoring.

6. Actively monitor the development of **NIST OSCAL**.
Summary

MEDINA aims to facilitate adoption of EUCS, specifically for automated monitoring, while paving the road for continuous certification.

Is EUCS’ automation the silver bullet in cloud cybersecurity certification?

Can MEDINA and OSCAL be game changers in the cybersecurity audit/certification practice?
Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com