Understanding Service Level Agreements in an AVCDL Context

Revision

Version 2
4/22/24 2:08 PM

Author

Charles Wilson

Abstract

This document describes how the service level agreements (SLAs) are considered within the context of the **AVCDL**.

Audience

The audience of this document are the cybersecurity development lifecycle practice leads who will be guiding **AVCDL** adoption within their organization.

Note: This document is not subject to certification body review.

License

Overview

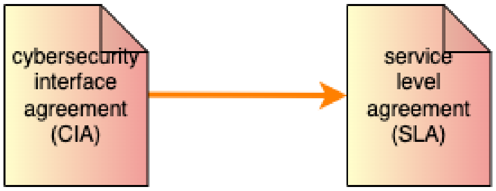
Although the **AVCDL** [1] does not specifically discuss the topic of service level agreements (**SLA**s), it was designed with the intent that there be provisions in place between the supplier and customer to ensure that critical cybersecurity activities are able to take place. This document will discuss the cybersecurity contributions to the supplier SLA.

SLA Ownership

It is important to remember that a supplier SLA is owned and managed at the organizational level. Any contributions supporting cybersecurity requirements need to be added with consideration to their impact on the overall SLA and its management.

Relationship to Other Supplier Documents

The following diagram (from **Understanding Supply Chain Interaction in an AVCDL Context** [2]) shows the relationship the SLA has with other supplier documents.


cybersecurity interface agreement (CIA)
service level agreement (SLA)

As shown above, the SLA is derived from the supplier cybersecurity interface agreement (**CIA**) [3]. This dependency allows the consideration of the specific requirements and responsibility division between the supplier and customer.

Cybersecurity SLA Items

The following is a list of cybersecurity-related items that should be considered for inclusion in the supplier SLA.

Note: This list is not intended to be the totality of cybersecurity items which might be included.

Note: The order of the following items is not intended to convey relative importance.

Identified Issue Reporting

It is critical that issues identified by the supplier are communicated to the customer in a timely manner.

Audit Support

Provisions need to be in place to accommodate all aspects of auditing required by the customer or regulatory requirements.

Log Extraction

Explicit provisions should be made addressing all aspects of access to and extraction of cybersecurity information contained within supplied component logs.

Incident Triage

This item complements issue reporting. Issues reported by the customer to the supplier need to have guarantees regarding the timeliness and resource levels to be applied to them.

Update of AVCMDS Information

Given that continuous improvement in cybersecurity posture is integral to the AVCDL, it is implicitly expected from the supply chain. The supplier should be required to provide updates when there are substantive changes to their AVCMDS information.

Time to Address Customer Reported Issues

The time to address customer reported issues is of great importance. This is especially true the higher up the supply chain that the issue manifests.

SBOM Updates

As with AVCMDS updates, SBOM updates need to be reported. These have not only a cybersecurity impact, but also a legal one.

References

1. **AVCDL** (primary document)
2. **Understanding Supply Chain Interaction in an AVCDL Context** (AVCDL elaboration document)
3. **Understanding Cybersecurity Interface Agreements** (AVCDL elaboration document)
4. **Understanding Your Cybersecurity Vendor Contract** https://cyberreadinessinstitute.org/wp-content/uploads/CRI-Guide-4-Reviewing-and-Understanding-Your-Cybersecurity-Vendor-Contract.pdf