The MDS2 Form

Leveraging manufacturer-provided data to improve IoMT security

The Manufacturer Disclosure Statement for Medical Device Security, generally abbreviated MDS2 (or MDS²), gives healthcare providers important cybersecurity information so they can evaluate the security capabilities of their devices. In many cases, the MDS2 form is the best, or the only way to discern aspects of the device that have a serious impact on its risk and on how to best handle any issues that arise during operation.

Many HDOs find consuming the raw MDS2 form quite daunting, but with Asimily, HDOs can receive all the benefits that analysis of the MDS2 provides with no work on their part. That's because Asimily is the industry leader in collecting and analyzing MDS2 data, with the largest repository of MDS2s in the industry, and the ability for customers to submit their own. But collecting the MDS2 isn't enough: Asimily digitizes the form, and incorporates the data into all parts of the HDO's workflow.

Asimily Insight assigns a score to each answer in the MDS2 form based on its impact to the device's security. These scores are then aggregated together and are one of the sources feeding into Insight's "Likelihood" calculation, which measures the probability of successful exploitation. These answers are also used to determine the "Impact," or criticality of a device to the HDO.

Asimily ProSecure uses the information from the MDS2 form as one of the factors to generate risk reports for devices that organizations are considering for procurement. Since it can be a challenge for organizations to collect MDS2s from each vendor for all the devices they are considering, ProSecure acts as both a source of MDS2 data and a platform for integrating the data into a holistic process of evaluating the security of a device before it is connected to the network.

Example Information in MDS2 Forms

- How can the device be patched? Does it require physical access, or can updates be provided remotely? Can the operator install patches on their own, or does everything have to go through the vendor?
- Does the device store or transmit Protected Health Information (PHI)? If so, what measures does it take to keep such information secure?
- Does the device have anti-malware software? If not, can it be installed by the operator?

How Asimily Uses MDS2s

- To determine the exploitability of a potential vulnerability, as expressed by Insight's Likelihood score, which can be reduced by mitigations that may exist on the device.
- To understand the impact on the HDO that a breach could cause, which is affected by information contained in the form, for example if a device stores PHI without encryption.
- To inform the mitigation recommendations that Insight provides, as specific mitigations may require the device to support a particular configuration.
- In conducting pre-procurement risk analysis, which Asimily enables with the ProSecure module.