

Requirement number and definition: 2.1.1.d

1. Constraints:

We understand the need of having the firmware updated in every moment, but there are systems which is not connected to the internet in order to keep it safe against malicious activities.

1. Objective:

The original goal is to be secured and prepared for any known/new bugs or being protected from new malware/viruses.

Compensating goal: to be protected on weekly basis.

1. Identified Risk:

There is still a chance of not having the ability to protect in time if there is a new virus which found.

1. Definition of Compensating Controls:

All of our protecting tools are manually updated once a week after updates are downloaded a scanned before transferring into our safe inner network.

1. Validation of Compensating Controls:

Statistically, we can see that when the outer and inner network is not connected there is less chance of being exposed to malicious files, so we can have the chance of not being updated in real-time.

1. Maintenance:

Make updates on a regular basis on a specific time in the week, and if there is any major update with high risk, make another update (in addition).

Requirement number and definition: 5.2.a

-Same answer as above (2.1.1.d)-

Requirement number and definition: 8.1.3

1. Constraints:

There were times that we saw that there are applicative users which are running scripts and/or logged-on to some important interior software/systems/tool inside our teams. And when we removed those users, problems started and more alerts have shown.

1. Objective:

The main goal is eliminating users trying to sabotage in the company systems.

The compensating goal is having some time to fully investigate all user activity before removing it.

1. Identified Risk:

No risk, only a waste of resources.

1. Definition of Compensating Controls:

Disabling the user from logging to the network, and after full-examination of its permissions, remove it.

1. Validation of Compensating Controls:

Not relevant.

1. Maintenance:

Every user that need to be removed is disabled and then, fully analyzed for making sure there is no other uses of it. And only after that – being removed.