Safe Medical Cyber-Security Solution

Anonemis Research
Simenona Martínez
AnonemisResearch.com

Safe Medical Cyber-Security Solution

Procedure and Protocol

Safe Medical Cyber-Security Solution offers security monitoring software for patients with wireless implanted or wearable medical devices.

Cybersecurity is one of the upmost important concerns in an almost purely digital world, meaning that up-to-date and secure configurations are nonnegotiable.

Safe Medical Cyber-Security Solution offers peace of mind by implementing A.I machine behavioral monitoring, intrusion detections, quarantine servers, data backups, device data operations via an offline secure secondary server data collection and ongoing anti-virus configuration.

Safe Medical Cyber-Security Solution implements A.I machine monitoring, which tracks the device operations, user behaviors and alerts the user of a usual activity which is cause for concern.

When the A.I systems determines the presence of usual activity, it will transition the device into incognito mode, which will initiate the intrusion detection and protection procedures, in addition to switching the device to a secure secondary backup network server which is separate from the primary server in question, which could be compromised.

This protocol is a critical offensive response to a threat because it prohibits an attacker from the gaining further access. In the event of an intrusion, the medical device can use the backup server which is provided by Safe Medical Cyber-Security Solution.

During this process the medical manufacturer will be notified and data collection from the patient's device will not be affected but collected via the secondary server.

When the event is resolved that data input is transmitted back to the device for data consolidation. Upon completion, a primary report is then sent to the manufacturer, physicians, the cybersecurity division in law enforcement and an overview is sent to the patient which will revisit patient protocol for protecting data.

The methodology is important because it allows rapid and consistent monitoring of devices in real time in the case of malicious intrusions. This alert can be lifesaving.

Anonemis Research
Simenona Martinez
AnonemisResearch.com