To be Safe
Advanced Security

09/09/2018

A Leading Document for Cyber Testing of QSnet-Rhodium cameras

this document summarizes the testing document dated 09/09/2018.

This document is a reference document for the testing document dated 09/09/2018**.**

Further to the testing document from 09/09/2108, it proves Capabilities and in accordance with the above-mentioned testing document, rhodium cameras are protected and comply with the following sections**:**

1- Password hardening capability and configuring different password for each user with different authorization levels.
2- Password encryption in AES256.
3- Each first initial activation of a new camera requires powerful minimum 8 different characters password. camera is obligated in defining a new password at a medium to high level, at first activation. No option to leave weak password is available, a password must be 8 characters and have different symbols (lower case, upper case and so on).
4- There is an option to prevent the Rhodium cameras broadcasting out of the organization's network so the camera is limited only to the local LAN.
5- There is an option to prevent the Rhodium cameras to listen to an SSH prot, so we can avoid the possibility of a Back Door.
6- Further to section 5, this can prevent Botnet.
7- Hardening an Access list of Authorized/Unauthorized access from the network.
8- Ability Of working in an 802.1X protocol environment with Radius Server.
9- Ability Of working and Broadcasting with Https protocol and matching with SSL Key.
10- Loading Firmware to the camera can only be from the manufacturer site, any other firmware will fail to load.
11- All the above sections were tested simultaneously while the cameras were configured in a Milestone Expert Xprotect VMS recording System, and functioned Fully with all features .

Menashe Nachum - CEO

To Be Safe

• Office: +972547833018 • Mobile: +972547833017 • 8 Shmuel Shrira st. Rishon Lezion, Israel

Menashe.n@tobesafe.ltd