It is not easy for startups to gain a position in the automotive industry.  What has been your experience, and what do you see as the biggest challenge in getting to scale?

This is a trust-based industry. I think that a position is gained once you have proven your ability to deliver. OEMs and Tier 1 companies worry that what has been delivered at the POC stage will not meet their production requirements or will behave differently. For example, in the automotive field, unlike IT, your cybersecurity product has to have a minimal footprint and minimal compute resource consumption, in order to fit into a real automotive ECU. I think the biggest challenge is the ability to deliver an automotive-compatible product. In addition to this, the fact that we have a veteran leadership with a track record of delivering security products on a large scale is also a key factor in this industry. There is also the issue of how hungry the customers are for your products. Our philosophy is to provide products that answer a real market need.

Does cybersecurity need to happen inside the vehicle, or can it happen at the cloud level?

It is very simple. If you want to be able to protect passengers’ lives and do mitigation in real-time to stop an attack, you have to do cybersecurity inside the vehicle.

If you think there is one thing that is generally misunderstood about the technology path or timing of Autonomous Vehicles, what is it?

Cybersecurity equals safety. For us, cybersecurity became a safety issue from the moment we made our vehicles connected. But for the end consumer, who is not sitting in this room, cybersecurity will be a psychological barrier and a demand from the OEMs for driverless cars. When John Doe buys an iPhone, he knows that the government cannot extract data out of it. When he sees an autonomous vehicle, he will ask if it can be hacked.

How is cybersecurity handled within vehicles today, and how will that evolve over time?

Public efforts, such as the new ISO standards for automotive cybersecurity, and an industry-driven cybersecurity community, like Auto-ISAC, will improve automotive cybersecurity capabilities and readiness. Having said that, there is still a very long way to go. Some OEMs are still internally discussing basic security features, while others are already testing and integrating advanced solutions. With time, I believe we will see consolidation in the OEMs’ cyber roadmap, each integrating multiple layers of security – starting from secure boot, then the perimeter, networks and endpoint protection.

What do you think will be the challenges of the future for OEMs dealing with cybersecurity?

From my experience delivering cybersecurity to mass markets, a major challenge will be the ongoing management of the cybersecurity lifecycle. Without being well prepared for this, it becomes a painfully expensive issue the day after rolling out vehicles with security solutions on board.