ETSI - ESO Certification Considerations

Alex Leadbeater
Chairman TC Cyber
BT Group Plc

Bringing it all together

Certification Considerations

- Goal: Building consumer trust in IoT products through standardisation and certification.
- “Voluntary” certification: Need to build a culture of Security adds value and suppliers gain value by acting responsibly with user data.
- Any certification scheme needs to add value and not be a box ticking exercise.
- Whole lifecycle of the product needs to considered and possibility of use in different verticals.
- Fit for purpose - Industry wide development of the scheme through ESOs essential.
- Certification must not be a barrier to entry or EU innovation
- Standards development must be open to all and freely available once published.

Flexible Standardised Certification Framework

- Common elements for most verticals
- However, one size unlikely to fit all
- Sector specific requirements
- Multiple Certification levels and possible verticals identification?
- Technology will always out pace formal standards.
- NFV / Cloud, create on Monday, deploy by Wednesday, replaced next week
- Ensure secure by default methodology
- Near real-time certification?
- Many IoT products will be underpinned by Open Source software
- How do ESO ensure Open Source can fit into this framework?

Priorities

- Start with the simple and the obvious
- Secure by Default
- Create culture of security adds value.
- E.g. TC Cyber IoT Security work TS 103 645
- Co-ordinate work between ESOs
- Avoid member state or industry ESO shopping.
- ENISA has a key role in enabling this.
- Specific technical co-ordination panel?
- Must be open to all industry stakeholders.
- User Groups, Operators, Manufacturers, Regulators.