Question	Answer(s)
Huge investment is done in ERP e.g. HANA . How can this be leveraged for I4.0?	HANA as a DB is known for it's fast processing, this helps with real-time analytics, predictive scenarios and thereby also helps us with Big Data processing that we could get from integrating to IoT devices. This will eventually help businesses get the right level of visibility at the right times during business process execution & decisions can be then Data-Driven decisions
How about the interface of security aspects to other features such as quality, safety etc. are fulfilled?	Interfaces play an important role in IoT, while building API's we have to consider security aspects listing a few key ones below 1) Sanitize input 2)Have Short-lived Tokens 3)Have Strong authentication in place 4)Enfore Standard Authorization for every endpoint 5)TLS transport encryption
How to find out whether the industry has machines that are compatible for IOT infrastructure. ie how do you distinguish legacy vs IOT machines/devices?	Industrial IoT systems have several legacy OT (operational technologies) like SCDA (Supervisory control and data acquisition),PLC(A programmable logic controller),DCS(Distributed Control System) BMS(Building management system), ICS (Industrial Control Systems) and many other manufacturing systems. Industrial IoT supports various protocols data sets and work with these manufacturing /legacy systems.
Any industrial standard has been released to achieve security in IOT systems?	https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/iot.pdf

How can we measure the security culture inside the organization? Is there any metrics which we can use to identify and improve the security aspects within the organization?	There are multiple ways to measure the security culture of an organization. Few companies measure security culture by performing mock email drills with few links and social engineering calls. And the other factors from the business side is the effectiveness of KPI's with respect to number of security issues reported vs the response and the fixing time.
Can you provide a case study describing layers of security is provided effectively in a industrial set up as well as consumer set up.	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
How much percentage of investment is required for organizations towards this cyber security approximately?	As per the experts, must be at least 5% of total expenditure but it also depends on the size IT investment of the organization. and the sector Ex: Health care has to follow regulatory
My question relates to BoL security. What is the difference between Authentication, Access Control, Confidentiality? To me, these multiple security requirements apprear to be the same.	Authentication- Process of verifying the identity of a resource or a person. This is in several forms Something you know- Phrase, Pincode, password, etc. Something you are- Passport, Smart card, Token, Id Card Something you are- Biometrics, IRIS, facial expressions Something you do - Signature, pattern Somewhere you are - country, Location, Network Access Control- That Regulates who or what can view or use resource or a place, and the permissions offred are authorizations. We have tseveral types of access controls. RBAC- Role-based access control DAC- Discretionary access control and MAC- Mandatory Access Control Role based Access Control Confidentiality - Data / Resources protected against unauthorized access limiting access to places or devices based on a set of rules

How Data quality be measured & secured?	Data is fuel for business in the digital era, we can consider the quality of the data by a few characters Accuracy, availability, and accessibility to the required set of people. At the same time data has to be relevant and reliable by maintaining the integrity of the data. At an organizational level, data security starts with Employee Awareness & at the same time having data centric security strategy.
What is the toughest security problem you came across but felt a tough nut to crack?	Humans are the tough and soft nuts to crack when it comes to security
Is any standard design being design in the world for industrial IOT systems?	There are quite a number of standards available for IoT security systems from NIST, ENISA and So on -> https://www.iotsecurityfoundation.org/ ->https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain
Is there are forum or websites where government publishes and updates the latest general cyber security threats in India on a daily basis?	https://www.cert-in.org.in/ They post latest security alerts on their website
Where is cybersecurity team layered.. w.r.t to Development & Q.A Team?	Devsecops is the way moving forward and it is about introducing security from the early stages of development. In this approach Developers and the QA team need to work hand in hand. security layered approach that is defence in depth is the model teams have to focus on rather than the team layered approach .