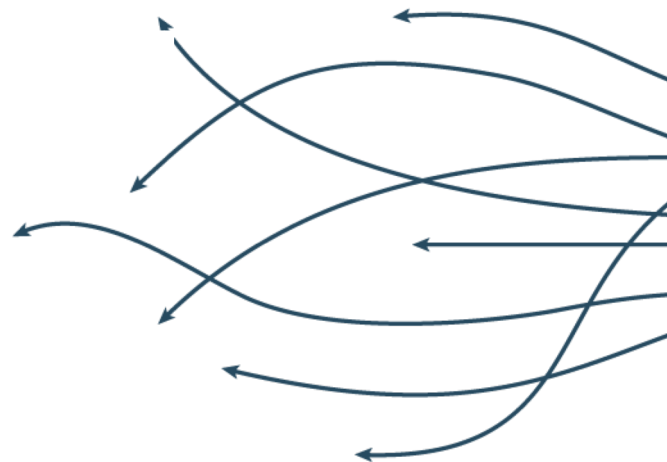


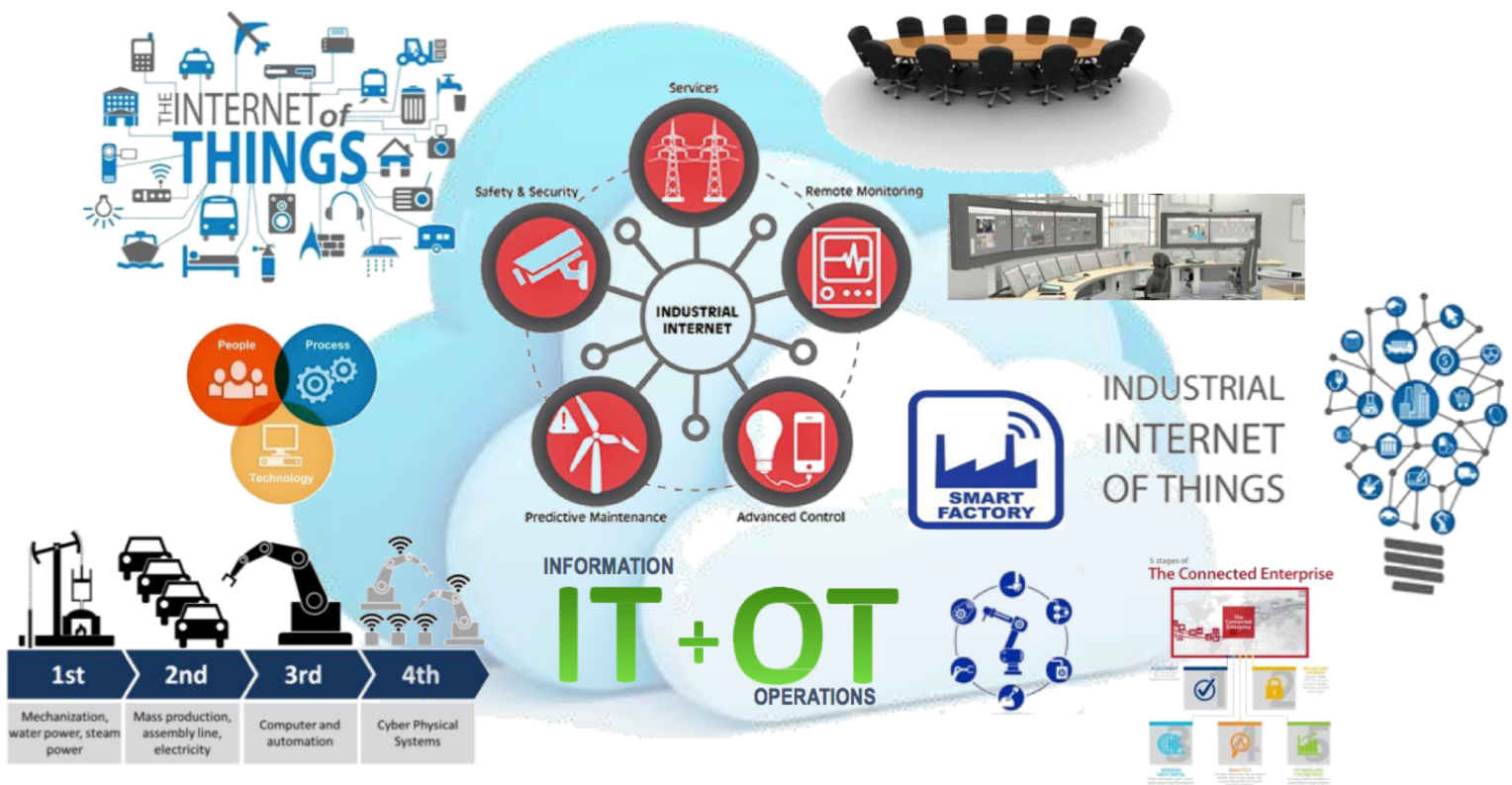
WHY I(OT) NEEDS A SOC



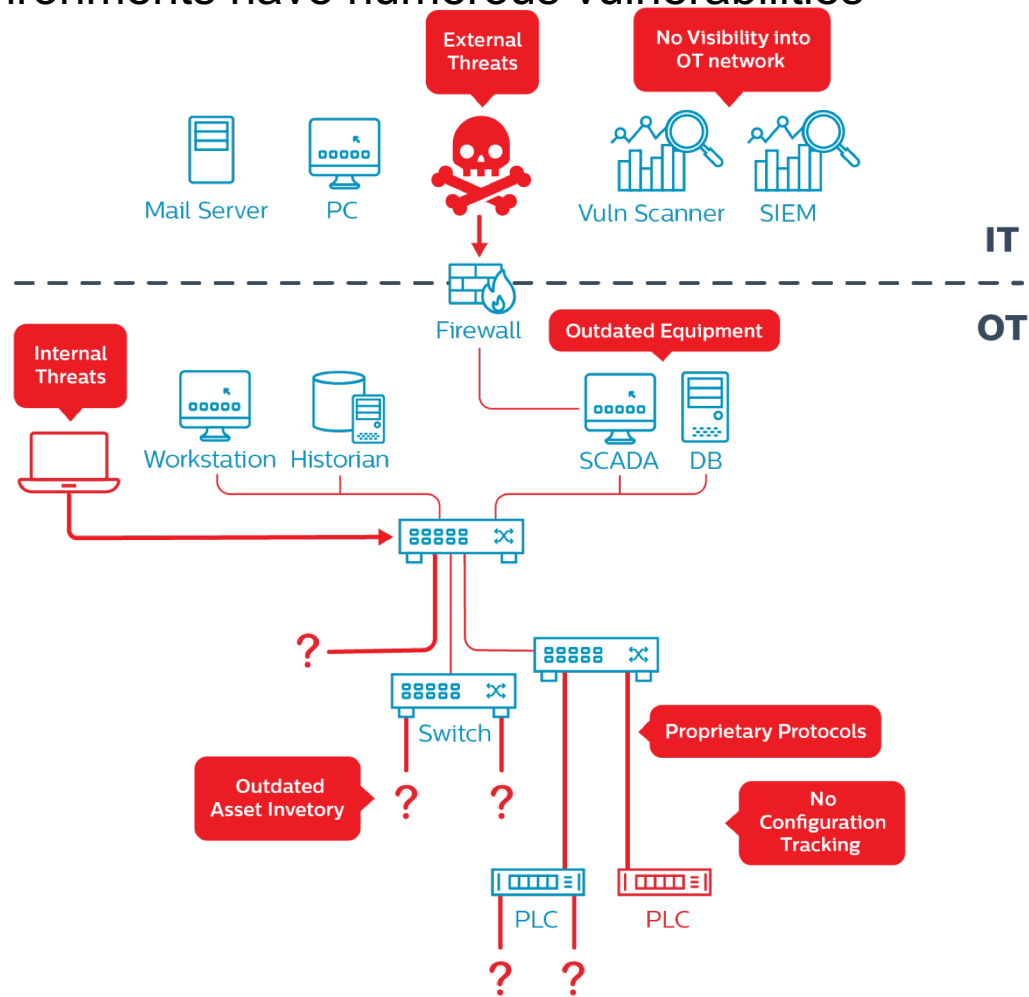
Pekka Puska
IBM Security Services Sales Leader



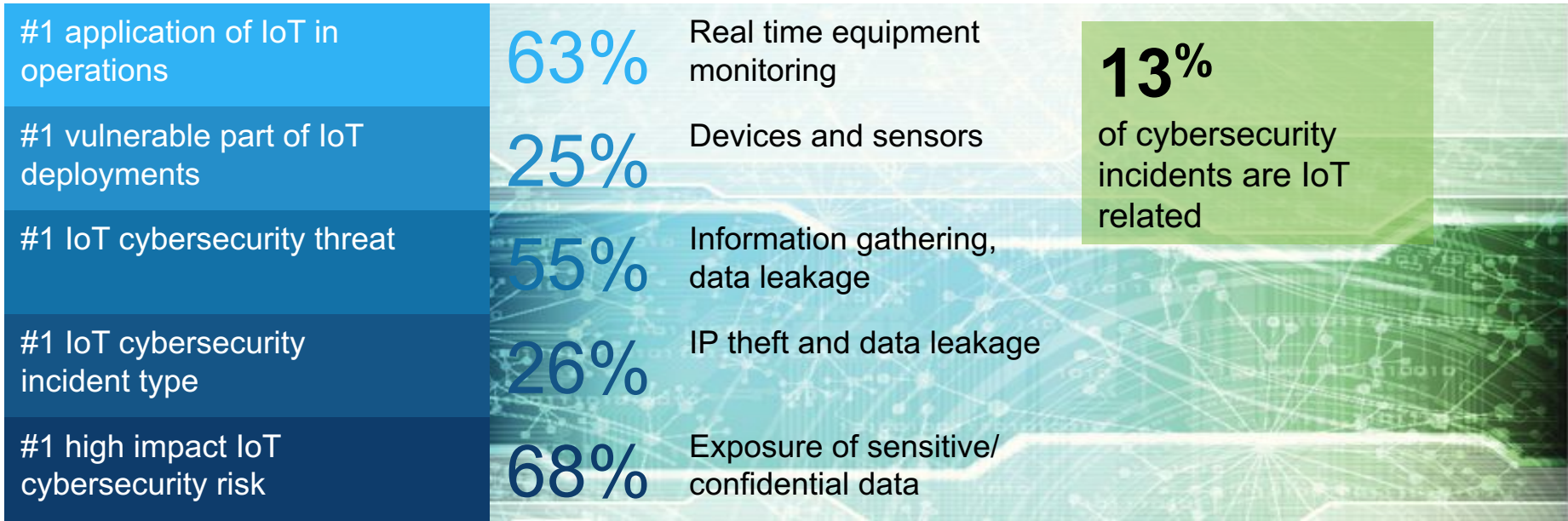
Evolution has led us to the connected OT environment:



OT and IOT environments have numerous vulnerabilities



The IoT is widely adopted in operations of industrial and utilities, exposing them to cybersecurity risk



n = 700

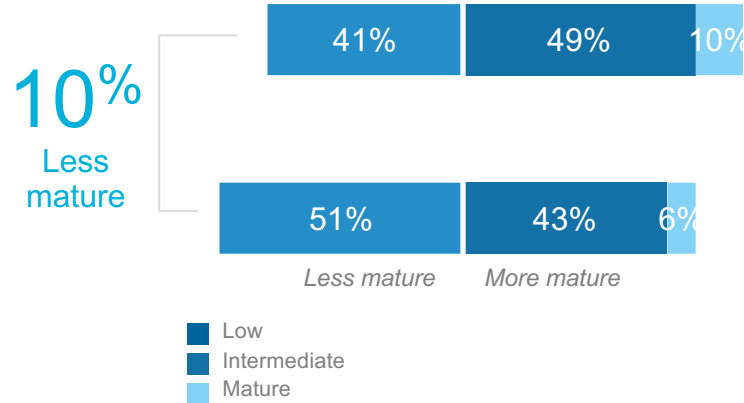
Source: IBV Benchmarking Program, 2018

...but they are not securing IoT in their operations at the same rate that they are adopting it

Comparison of the maturity of organizations' IoT capabilities with the maturity of the cybersecurity capabilities in place to protect them

IoT capability maturity

IoT cybersecurity capability maturity



*"As companies continue to embrace a platform approach to the IIoT, **it is critical that industrial cyber security capabilities are embedded as part of the platform foundation**, and not considered add-on pieces of functionality."*

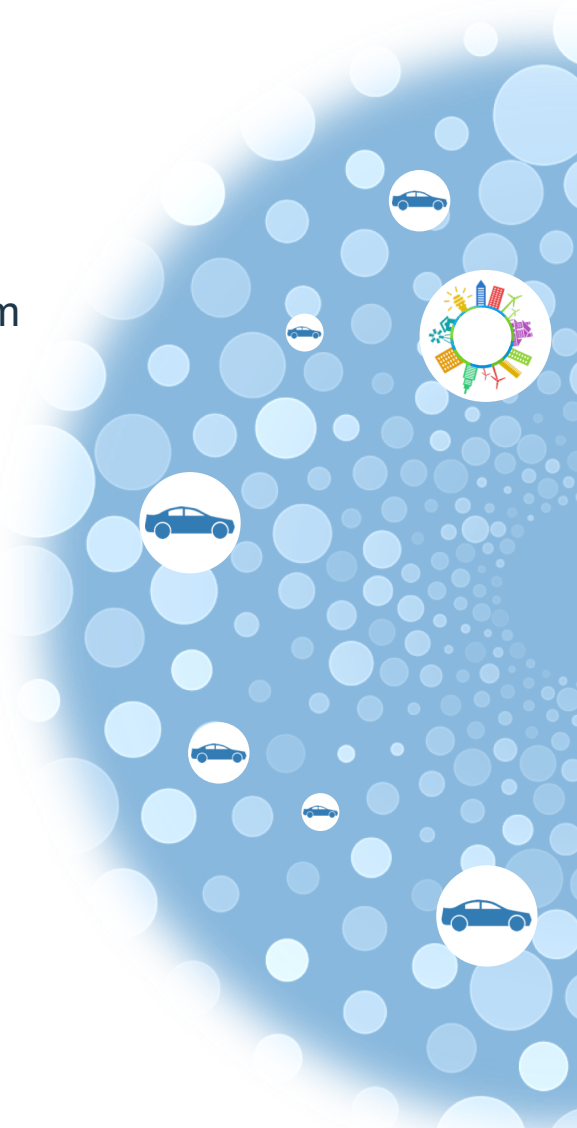
Source: IBV Benchmarking Program, 2018; Putting industrial cyber security at the top of the CEO agenda", LNS Research, 2017, <http://www.lnsresearch.com/research-library/research-articles/-ebook-putting-industrial-cyber-security-at-the-top-of-the-ceo-agenda>; n=700

Source: IBV Benchmarking Program, 2018

IBM Philosophy: Bringing Security Intelligence to IoT World

KEY CHALLENGES

- Advanced real-time monitoring capability of the complex platform
- The ability to collect security data from the edge
- Extensive analytics capabilities that cross-correlate data from different sources so as to identify hidden threats
- Risk-based threat management capability



IOT security does not differ so much from IT security, but there are some important differences to understand...

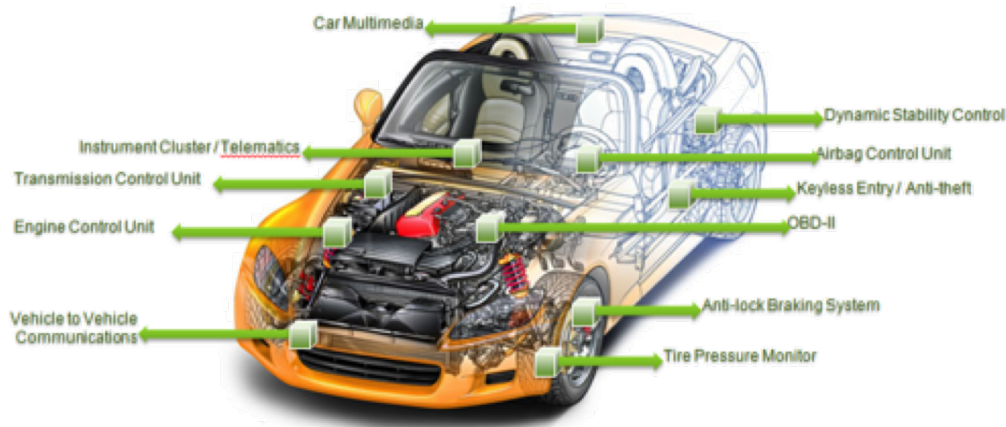
Impact of disruption

IT attacks

- Data loss
- Business disruption
- ICAP/IP loss

OT attacks

- Human & environmental harm
- Process interruption
- Process manipulation



Automation is more present in IOT environments

Log sources are often simpler and sometimes more mobile in IOT environments. Different standards

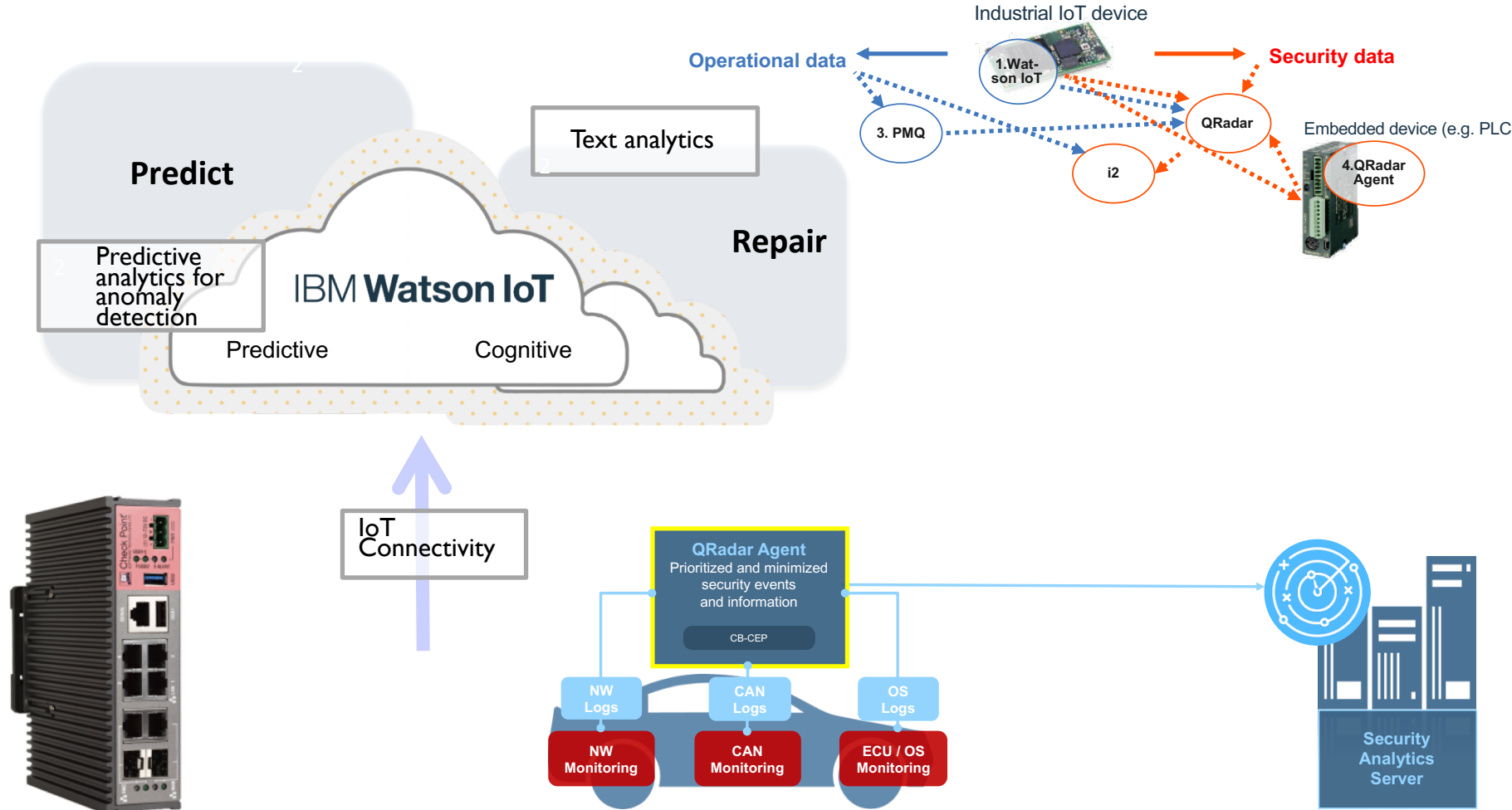
Individual logs are less informative in IOT environments

Big Data is often the foundation of the IOT - platform

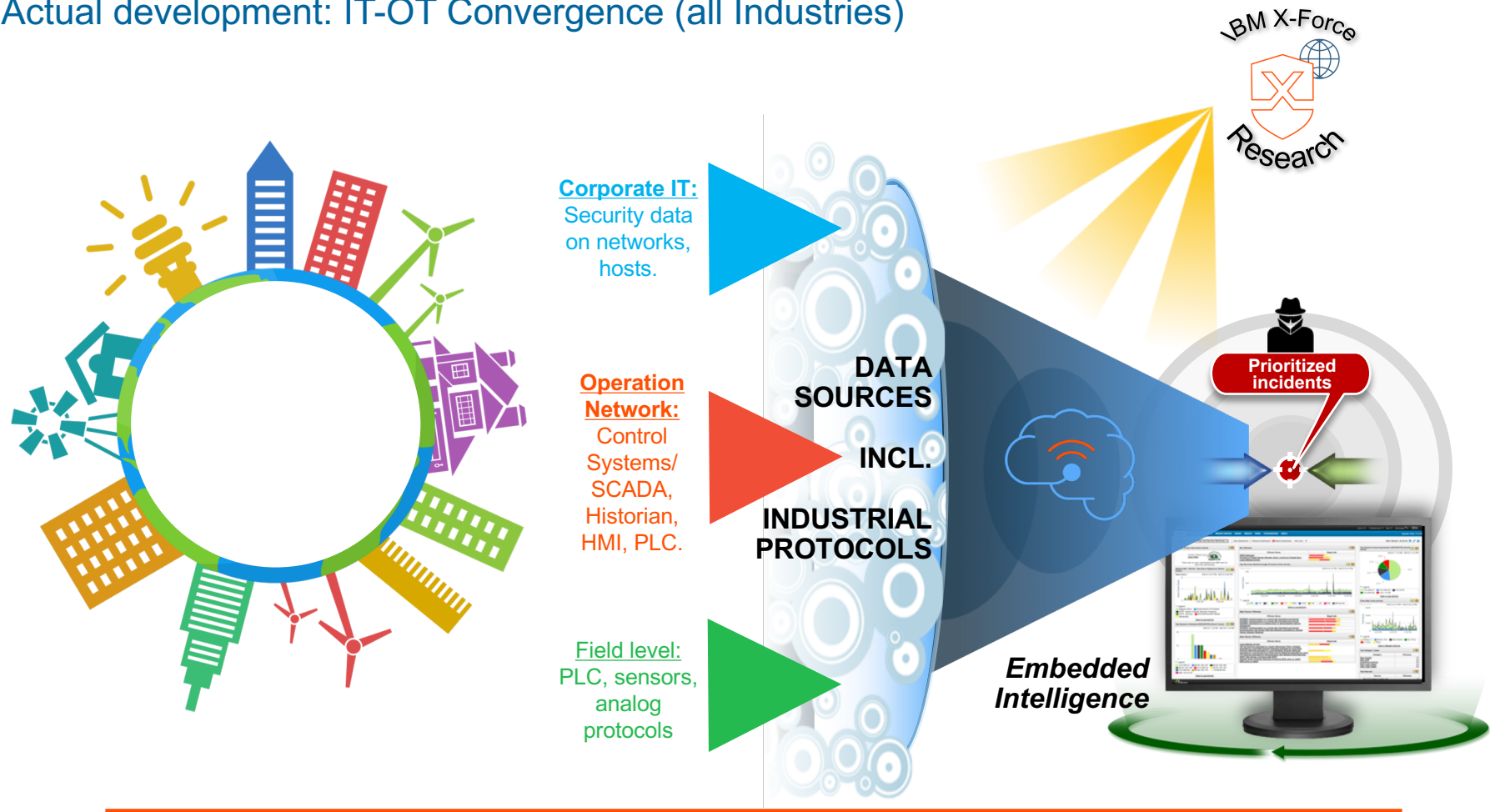
The criticality of an IOT environment often supersedes the security level of the equipment installed

Flow can be leveraged, but is less informative

Data Normalization – multiple flavors of...



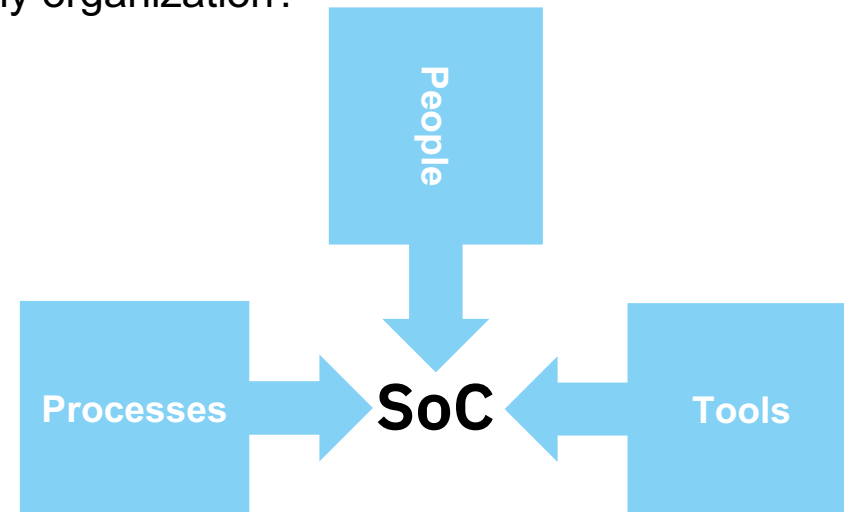
Actual development: IT-OT Convergence (all Industries)



Event Detection is only the Beginning

More information is needed to obtain actionable data




- What is the alert priority based on risk assessment?
- What was the attack chain (entry point, lateral movement and exploit)?
- What vulnerabilities were exploited in this attack?
- What are the similar attacks seen in the past?
- What is the level of exposure to this attack in my organization?
- What was the attacker's objectives?





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/@ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.