

MY BACKGROUND IN IOT

- 23 years in Cyber Security
- Current Canadian Chair of ISO/IEC SC 27 Information Security
- International Convenor on Trustworthiness to ISO/IEC SC 41 on IoT and Related Technologies
- Editor for ISO/IEC 27030 on IoT Requirements for Security an Privacy



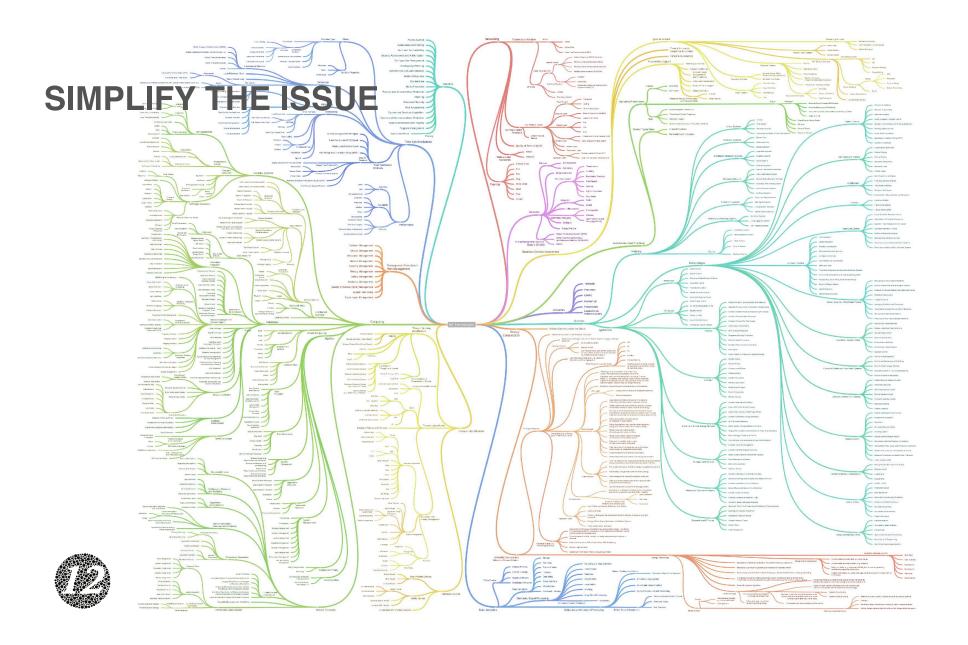
THE PROBLEM Cloud Database Database Hackers, State Sponsored Threats, and other cyber criminals Platform API

WE NEED A WAY TO "QUANTIFY AND MITIGATE RISKS" AS VENDORS, BUYERS AND CONSUMERS OF IOT TECHNOLOGY

Threat Visibility



No Threat Visibility



APPROACH TO THE PROBLEM

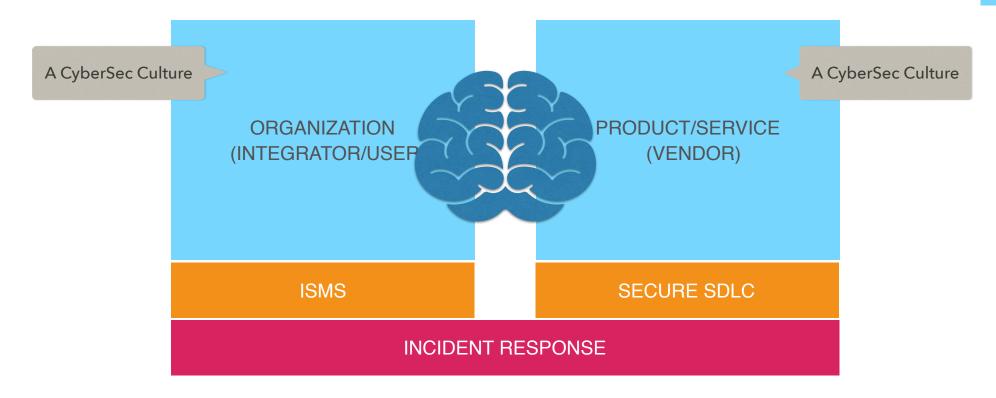
ORGANIZATION (INTEGRATOR/USER)

PRODUCT/SERVICE (VENDOR)

COMPETING PRIORIES TO RISK AND REQUIREMENTS



STANDARDS VIEW TO THE PROBLEM





APPLICABLE STANDARDS

ORGANIZATION RISK

ISO/IEC 27001 - ISMS

ISO/IEC 27034 - APPLICATION SECURITY

ISO/IEC 27018 - CLOUD SECURITY

ISO/IEC 27030 - IOT REQUIREMENTS***

CRYPTO, TESTING, NETWORKING, PRIVACY

PRODUCT/SOLUTION RISK

IEC 62443 - IIOT

IEC 30141 - IOT RA** (TRUSTWORTHINESS)

ISO 27799 - HEALTH INFORMATICS

IEC 61508 - FUNCTIONAL SAFETY

ISO/IEC 15408 - CC FOR GOVERNMENT



GOAL: MITIGATING RISKS TO COMPANY AND PRODUCTS BEING DEVELOPED

IoT Security: Using Standards as the Baseline

HOW TO USE STANDARDS

- 1. Quantify Risk(s) {both vendor and buyer}
 - TRA, Threat Modelling, Gap Analysis, Testing, and Evaluation
- 2. Deploy a ISMS {both vendor and buyer}
- 3. Deploy a Secure SDLC {vendor only}
 - Ensure all processes/procedures and products follow this guidance
- 4. Defects {both vendor and buyer}
 - a. Product/Solution via testing {Cert, Pen Testing, VA's, etc}
 - b. Organization via audit and assessment
- 5. Aim for continuous improvement {both vendor and buyer}

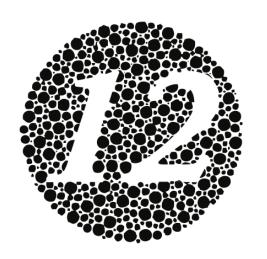


WHY USE STANDARDS

- 1. Can certify product and organization under ISO and IEC
- 2. Recognized globally
- 3. Provides the necessary "proof" of due diligence
- 4. Provides **assurance** to buyer that product has been designed, tested and evaluated
- 5. Meets or exceeds minimums typically requested for compliance



THANK-YOU FOR YOUR TIME



faud.khan@twelvedot.com @encrypto99 +1 613 447 3393

www.twelvedot.com

