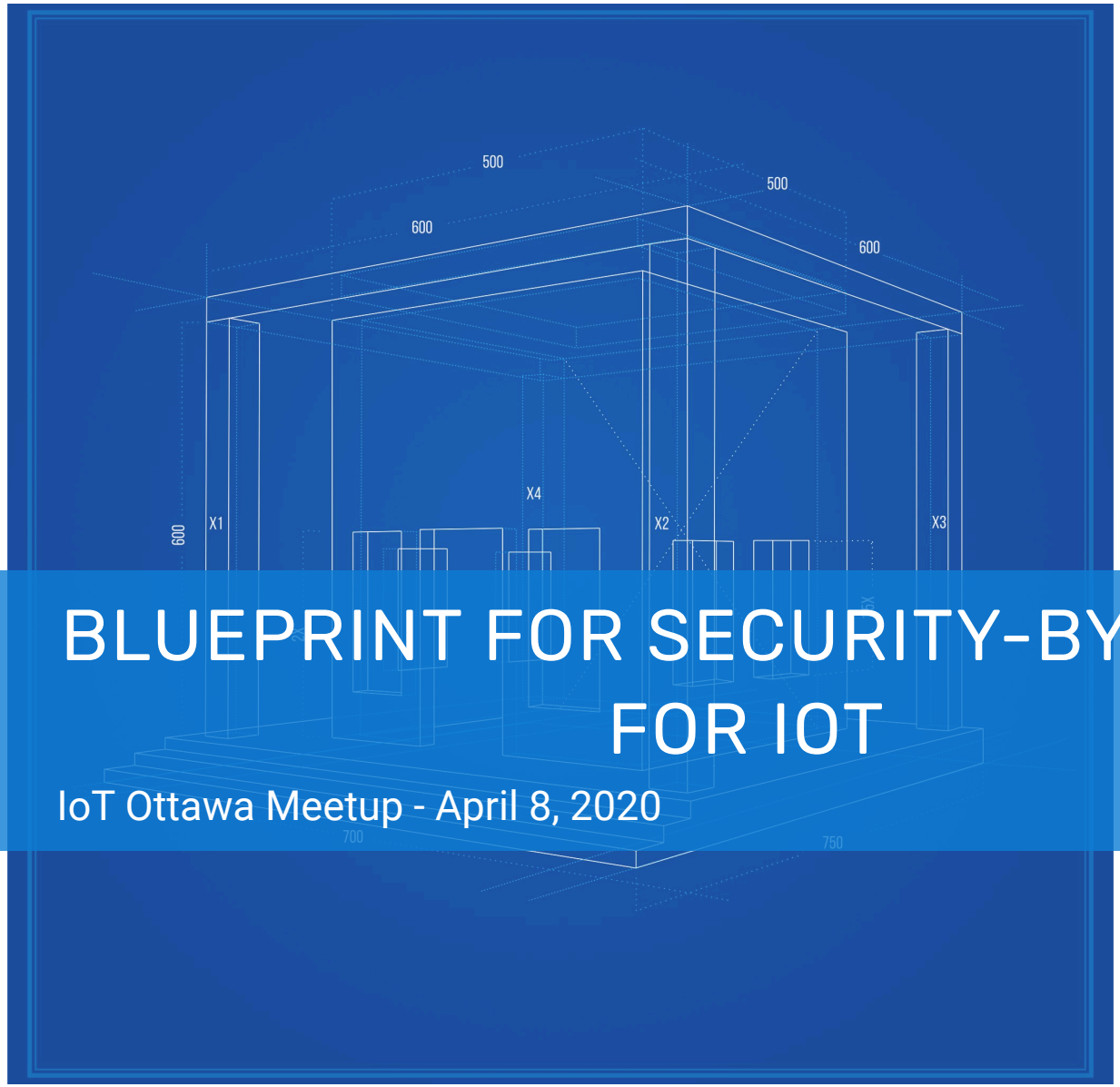


BLUEPRINT FOR SECURITY-BY-DESIGN FOR IOT

IoT Ottawa Meetup - April 8, 2020

DESIGN. BUILD. SECURE

AGENDA

- Industry Trends
- Approach to Business
- Approach to Development
- Understanding the Role of Standards
- Goal of a Cyber Program

ABOUT TWELVEDOT

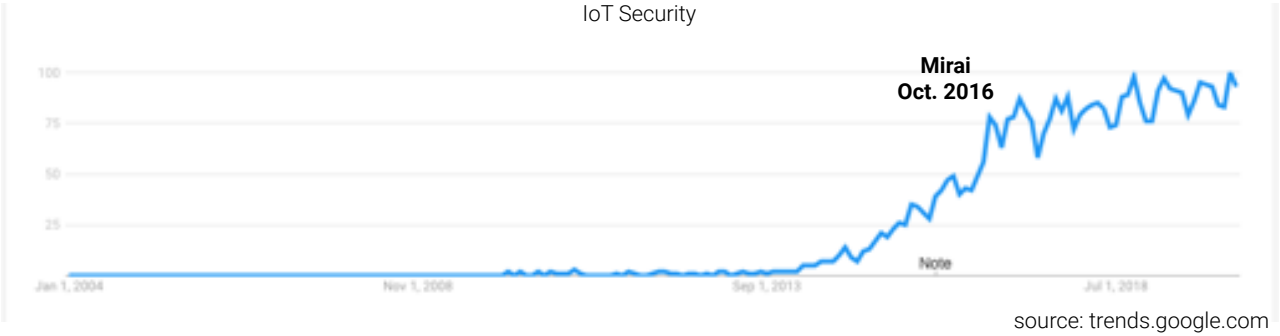
- We work CSA Group for testing, assessment and standards development
- Editor for ISO/IEC 27030 IoT Security and Privacy
- Editor of ISO/IEC 30149 IoT Trustworthiness
- Internet Society Multistakeholder Process for IoT Security and Privacy - Chair of the Labelling WG
- Internet Society IoT Platform Member
- We have pen tested and evaluated well over 500 IoT products to date
- Work with companies to improve both products and organizations

SOLUTIONS ABOUND

Home, commercial, healthcare, smart city, smart manufacturing……

IoT products have and will continue to enrich our lives and provide means for all citizens to live better lives.

TRENDS - ATTACK AND ATTACK SURFACE



source: trends.google.com

source: trends.google.com

MIRAI SOURCE CODE

```
char recvbuf[128];
struct sockaddr_in addr;
int sfd, ffd, ret;
unsigned int header_parser = 0;
int arch_strlen = sstrlen(BOT_ARCH);

write(STDOUT, EXEC_MSG, EXEC_MSG_LEN);

addr.sin_family = AF_INET;
addr.sin_port = HTONS(80);
addr.sin_addr.s_addr = HTTP_SERVER;

ffd = open("dvrHelper", O_WRONLY | O_CREAT | O_TRUNC, 0777);

sfd = socket(AF_INET, SOCK_STREAM, 0);
```

NEW EXPECTATIONS

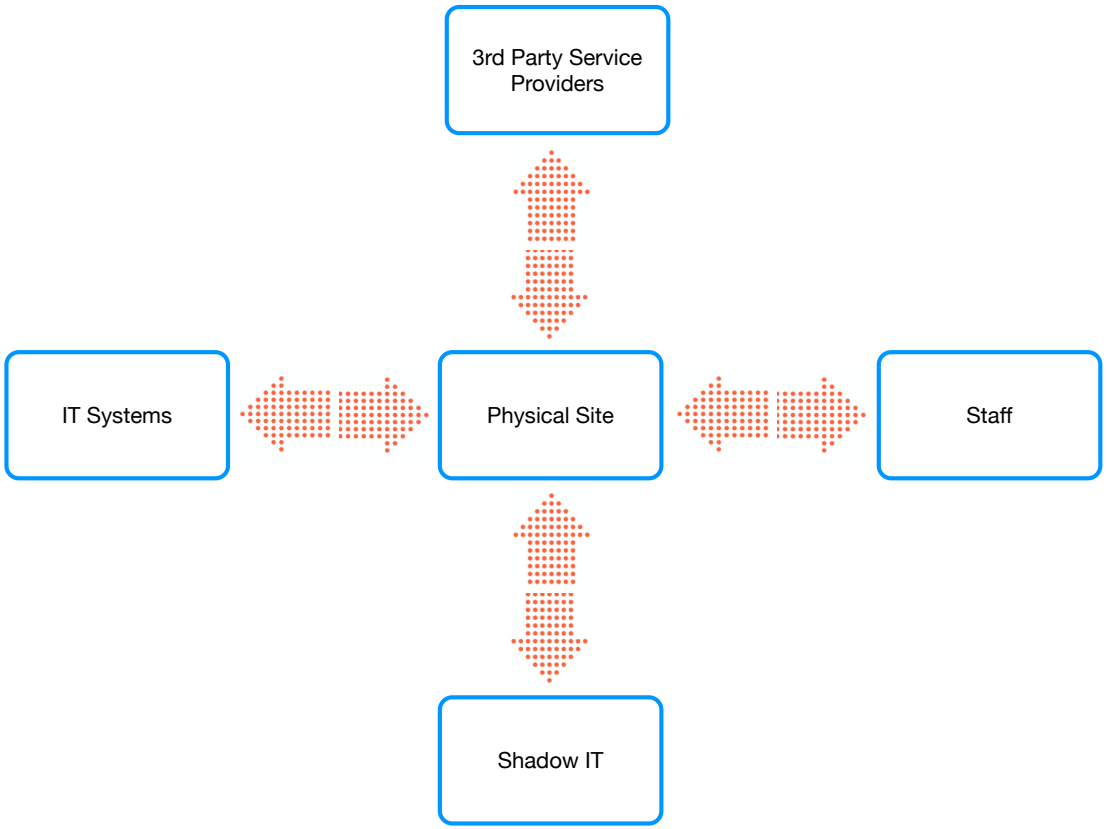
- Many nations are developing regulatory and certification requirements
  - Japan, United Kingdom, EU, and Australia
  - Canada will not develop one but probably adopt another nations framework
  - CSA EXP-T200 (Bi-national standard) being developed
- Several provinces are looking at requirements for products in specific sectors
- Many associations are developing methodologies to help (IoXT)
- NIST and ISO working on Baseline standards to support SMB vendors

NEW APPROACH

- Need to think of this as two broad aspects:
    1. Organization
    2. Software development lifecycle
- Implementing **security-by-design**
- Will provide an auditors approach and show later how all of this relates to standards
- Assume all security components and software is compromised. Now prove it is not!

ORGANIZATION

ORGANIZATION ATTACK SURFACE



IoT613 - Blueprint for Security-by-Design for IoT

ORGANIZATION APPROACH

- Need to quantify data being collected, processes, stored and destroyed
- Who has access to this data?
- What systems have access to this data?
- What would happen if this data got compromised?
- How is your development structured to understand potential risks to products?
- What policies and procedures need to created:

  a. Staff understand how to handle and process this data?

  b. Usage and deployment of systems and services

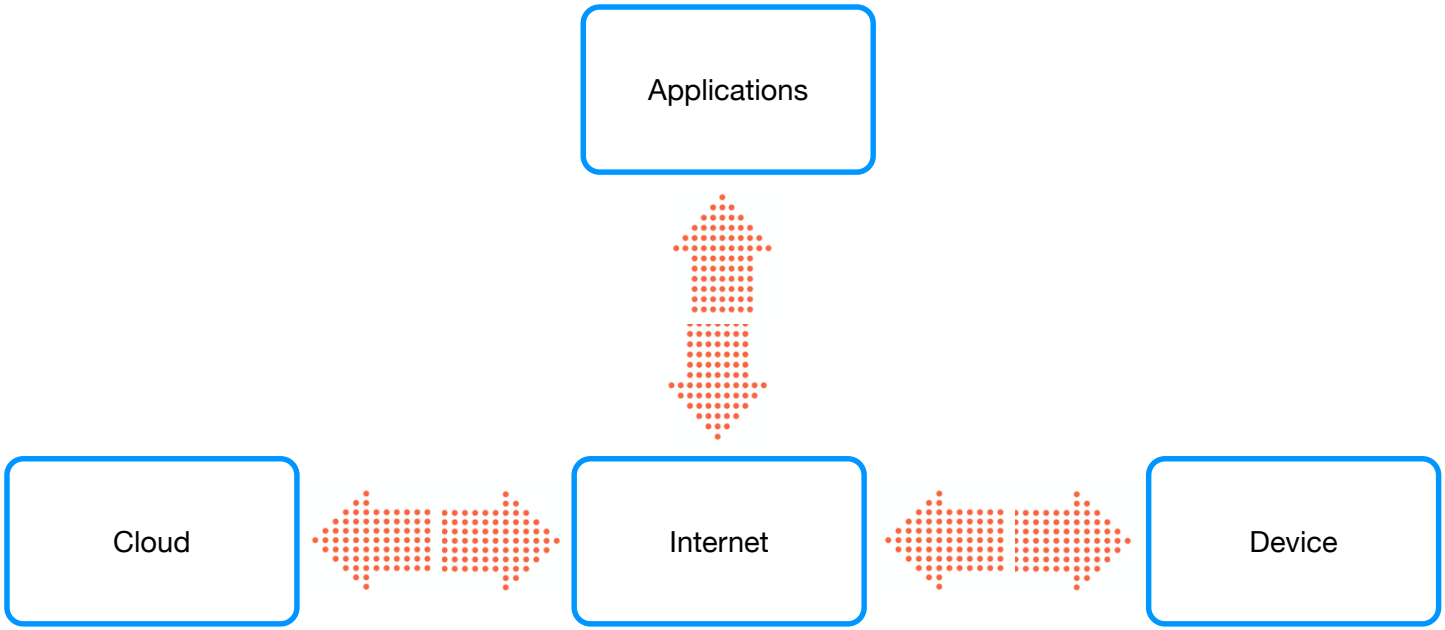
  c. Part they play in mitigating risk and reporting incidents

ORGANIZATION IMPLEMENTATION

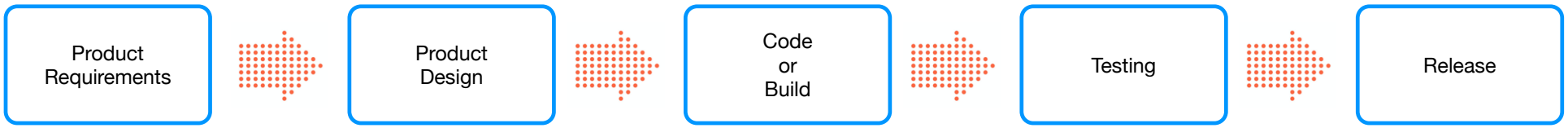
- Need to provide awareness training to staff to potential cyber risks for the company and products.
- Track current cyber risk landscape for changing risk aspects
- Update policies and procedures to mitigate on going risks
- Risk assess all new technologies and services being considered
- Document, document, document!

SECURE DEVELOPMENT LIFECYCLE (SDLC)

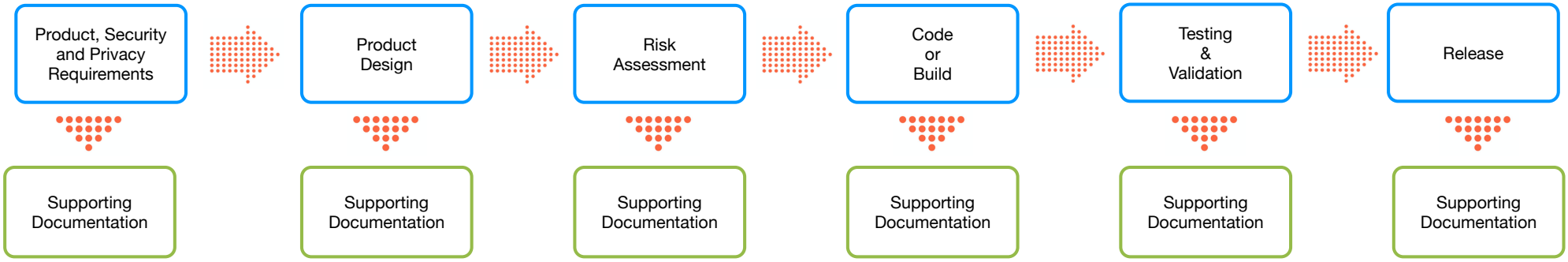
PRODUCT ATTACK SURFACE



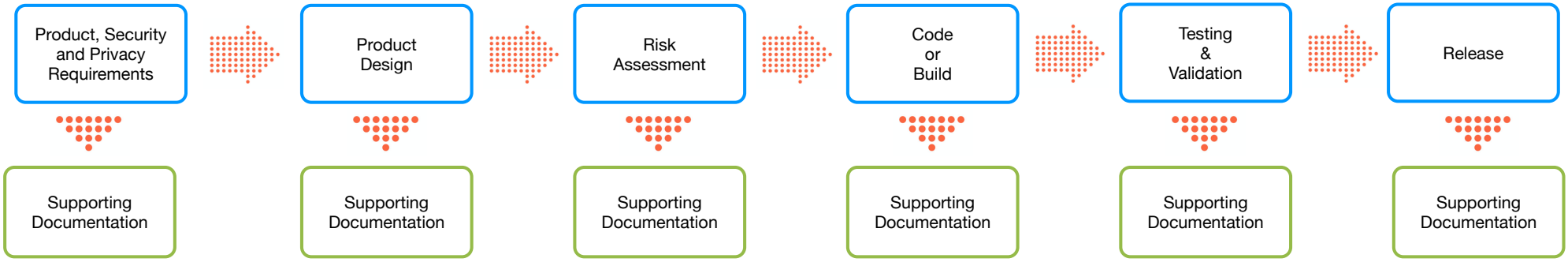
TYPICAL APPROACH TO DEVELOPMENT



SECURE APPROACH TO DEVELOPMENT



SECURE APPROACH TO DEVELOPMENT



HOW IS THIS RELATED TO STANDARDS?

LEVERAGING STANDARDS FOR CONTROLS

- Securing an company uses a method called Information Security Management System
  - ISO/IEC 27001 and family of standards (complex)
  - NIST 800-53 standard (complex)
  - COBIT, ITIL and others
- Securing a product requires implementing an SDLC
  - ISO/IEC 62443 series (industrial)**
  - ISO/IEC 27034 Application Security (complex)
  - NIST Frameworks Secure Software Development Framework (SSDF)
  - NIST Baseline Controls for IoT***

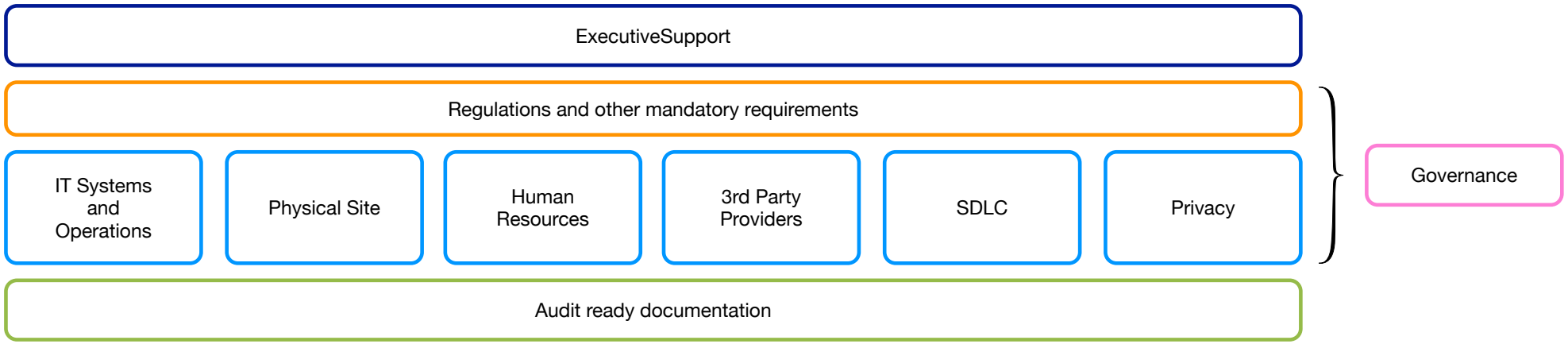
IOT SPECIFIC STANDARDS

- Association based standards
  - Industrial Internet Consortium (IIC)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Internet of Secure Things (IoXT)

- International Standards
  - ISO/IEC 27030 IoT Security and Privacy (currently under development)
  - ISO/IEC 30149 IoT Trustworthiness (currently under development)
  - To be named and started – IoT Baseline (based on NIST document)

YOUR GOAL

STARTING MODEL



START SMALL AND GROW THE PRACTICE

- Start small
  - Focusing on understanding the risks to your product/service
  - Focus on understanding the risks to your company
- Security test and evaluate your product to understand what a “hacker” sees
- Provide your staff training on the identified risks and how to prevent and report
- Always look to improve with new releases {no need to fix everything day 1}

OPEN DISCUSSION

Questions

or

Comments

Contact: security@twelvedot.com

DESIGN. BUILD. SECURE

security@twelvedot.com
@encrypto99
www.twelvedot.com