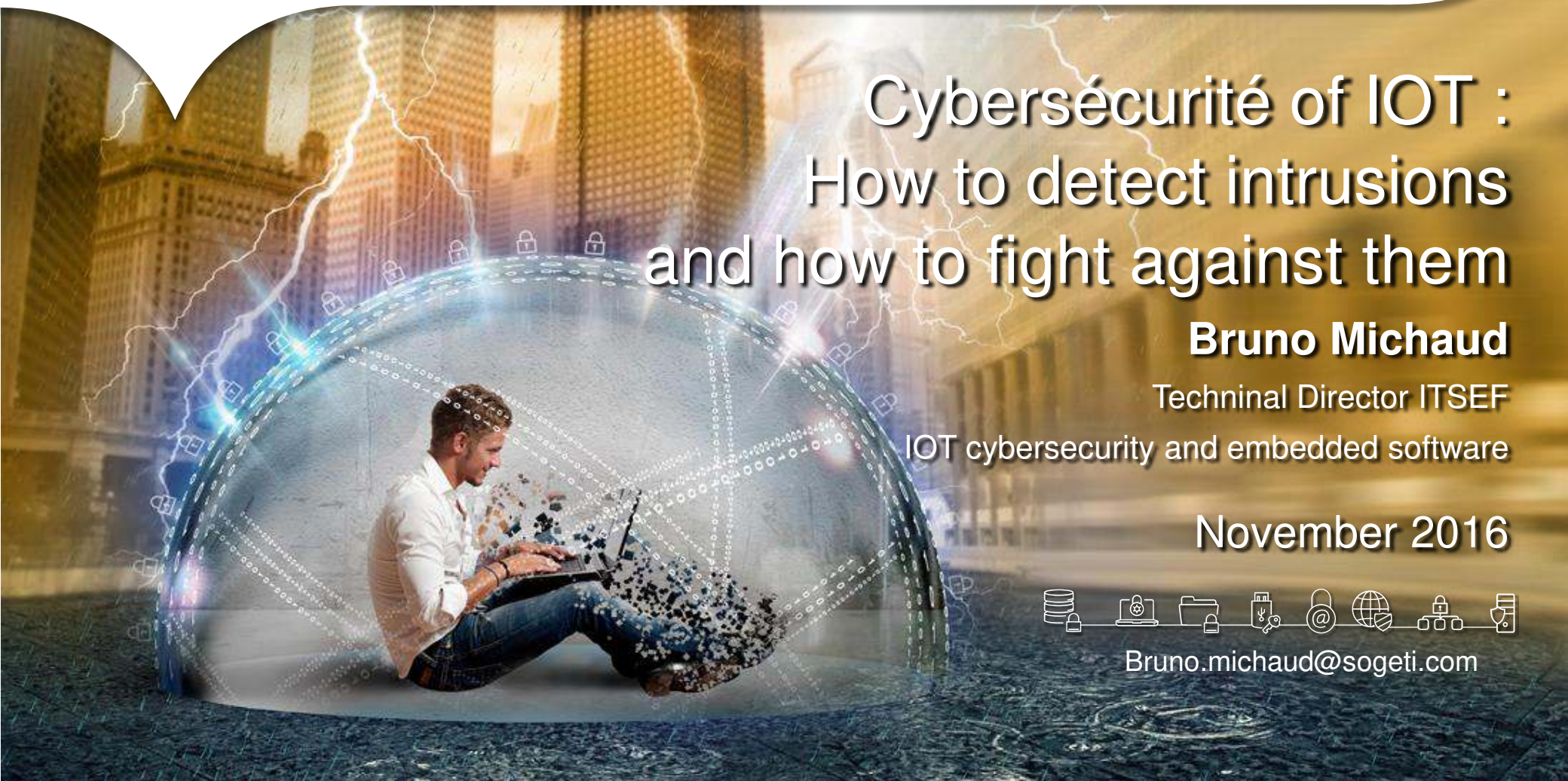
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI



Cybersécurité of IOT : How to detect intrusions and how to fight against them

Bruno Michaud

Techninal Director ITSEF

IOT cybersecurity and embedded software

November 2016

Bruno.michaud@sogeti.com

Table of contents

1.1 Position of the problem: IOT range

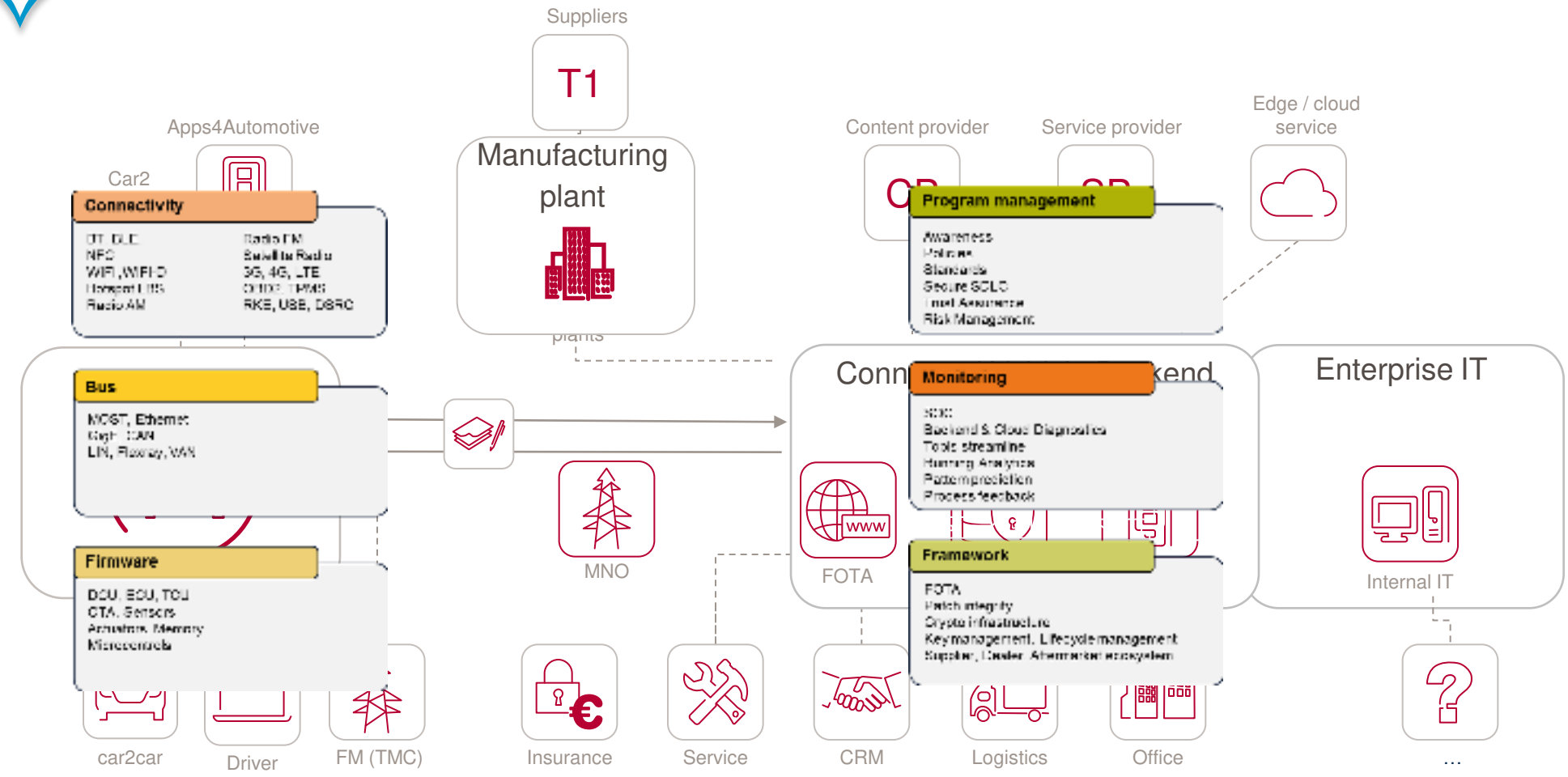
In addition to PC and IT systems that are not considered as IOTs, a lot of gimmicks or usefull objects are connected to the Internet :

- SmartPhones
- Watches
- Medical systems
- Vehicles
- Industrial Sensors
- Survey Cameras
- Light bulbs (Lifi)
- Raspbery boards
- Home systems …

1.2 Attack surface

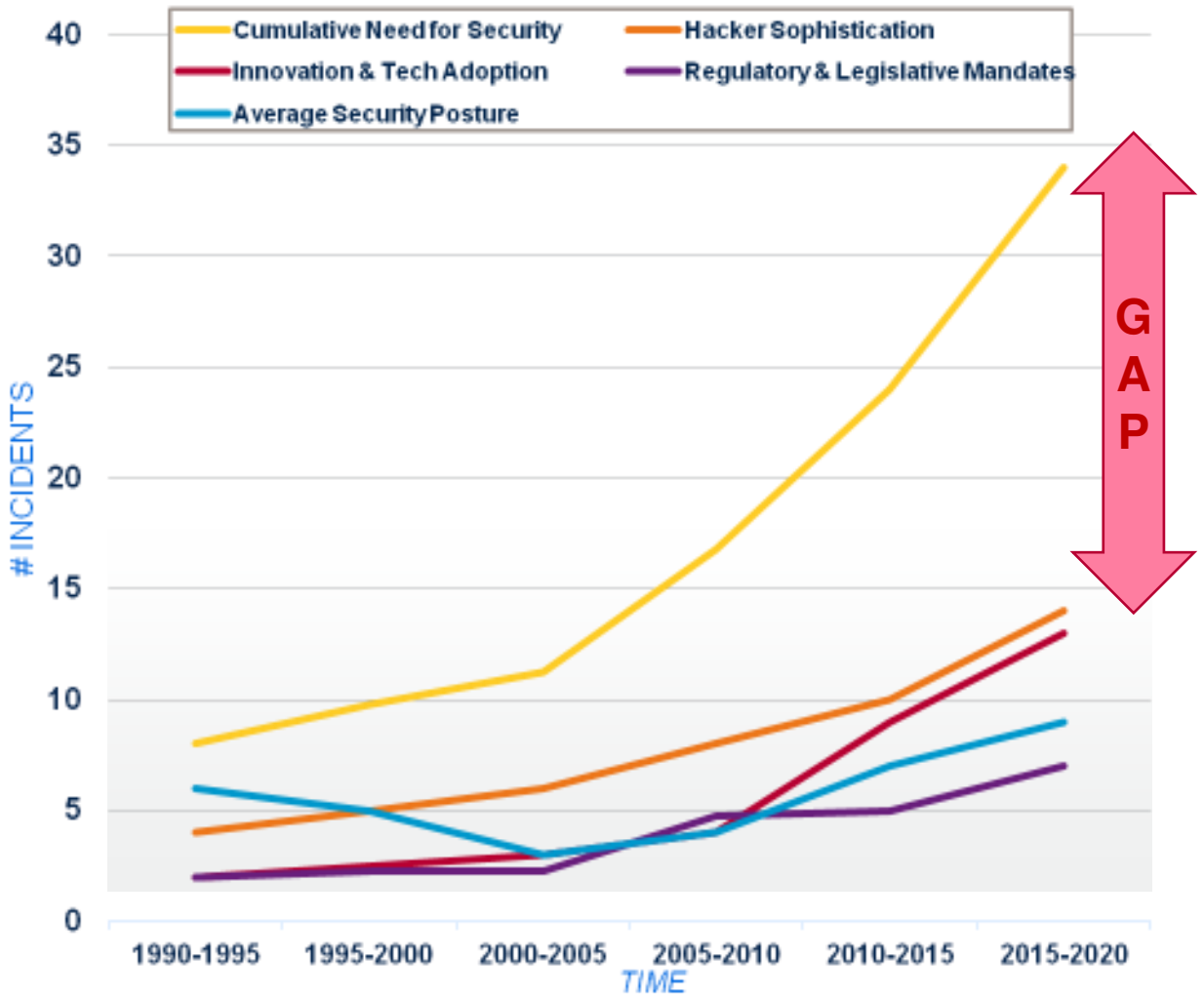
- Attack surface is the set of all the possible entry points that a hacker can use to penetrate a system:
  - Social engineering
  - Mails, attached documents
  - Protocols
  - Network equipment
  - Software Applications and implementation
  - Web browsers
  - Cryptography, key management,
  - Identity Management
  - Data Bases
  - Operating systems, virtualizations, containers
  - Hardware, including power supply, cables,
  - Radio communication and EM radiations, …

1.3 I.E. attack surface for a connected vehicle



Systems has become more and more complex (a BMW 7 series has 12 SIM cards).

1.4 Position of the problem: Security Trends



Source: Capgemini

Cybersecurity Key Trends:

The security gap is widening

- Despite the increase in spend & capabilities

Threats are cumulative

- Old, new & emerging

Technology surface expanding

- Many companies still have large legacy systems
- Cloud, mobile, global expanding
- Soft perimeter
- Exponential data growth

Current Culture not prepared

- Large Enterprises are compliance-driven in their Cybersecurity approach and culture is slow to adjust
- Boards are interested and accountable

2 Who and what to fight against ?

WHO	HOW	WHY	Type of attacks
STATES	All means	Politics,	DDOS, malware
COMPANIES	All means	Economic intelligence	Malware
ORGANIZATIONS	All means	Money, freedom	Malware, ransomware
ACTIVISTS	All means	Destabilization, influence	DDOS
HACKERS	Technology, engineering	Money, glory	ransomware

3 Incident detection

2 families of IDS :

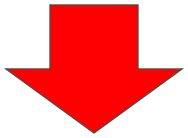
AMP based on signature

* Reputation

AMP based on comportemental :

•Code behavior
•Traffic behavior

But no Anti Malware Protection embarqued on most IOTs



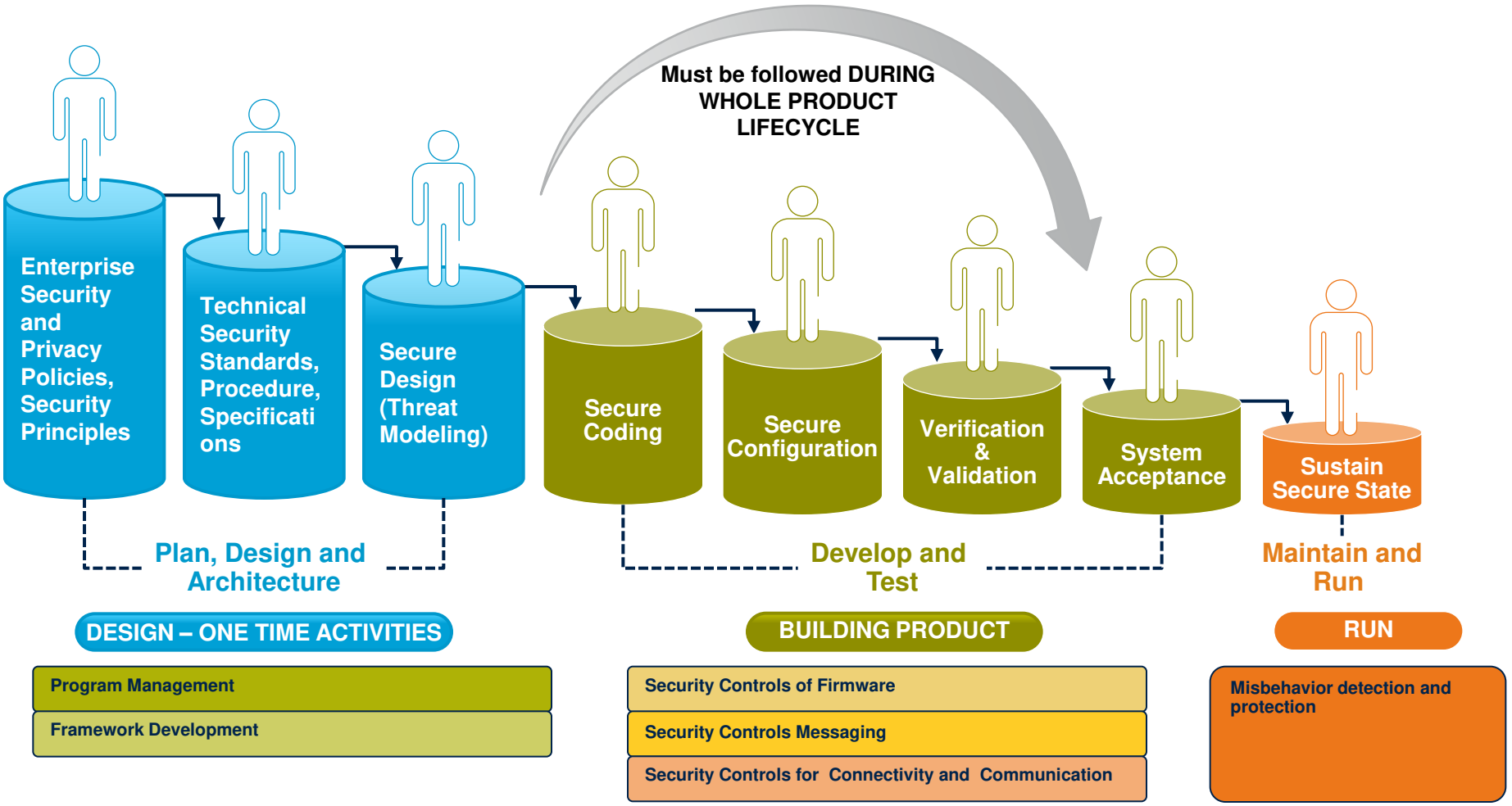
SECURITY BY DESIGN

4 Defense methods

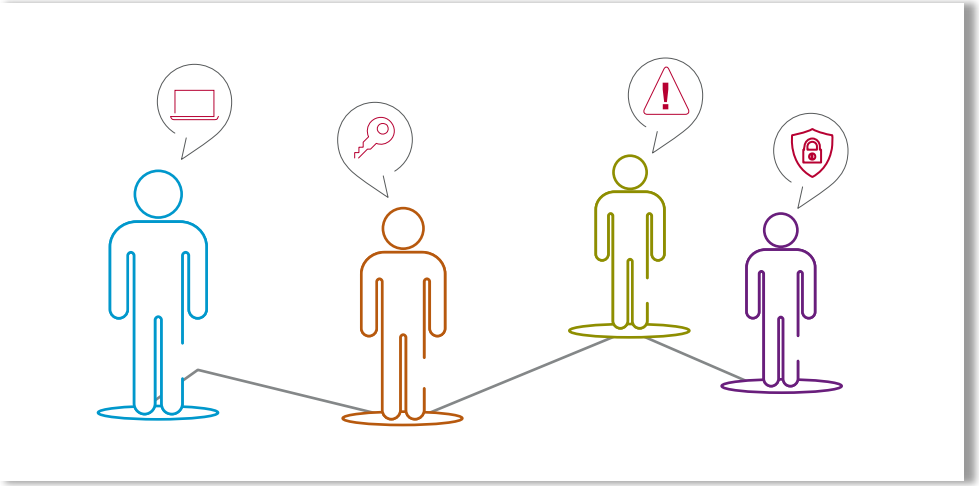
A few basics:

- Need to use proven methodologies on three levels:
  - **Human** : Security Strategy, Capabilities and operating models
  - **Processes** : risks analysis, risks management frame, Security policy
  - **Technology** :
    - Secure by **Design** (architecture, …),
    - Secure **Build**,
    - Secure **Run**
- Use proven concepts such as Defense in Depth

4.1 Secure Application Design, Delivery and Operations



4.2 THINK like a HACKER



CyberAttack LifeCycle

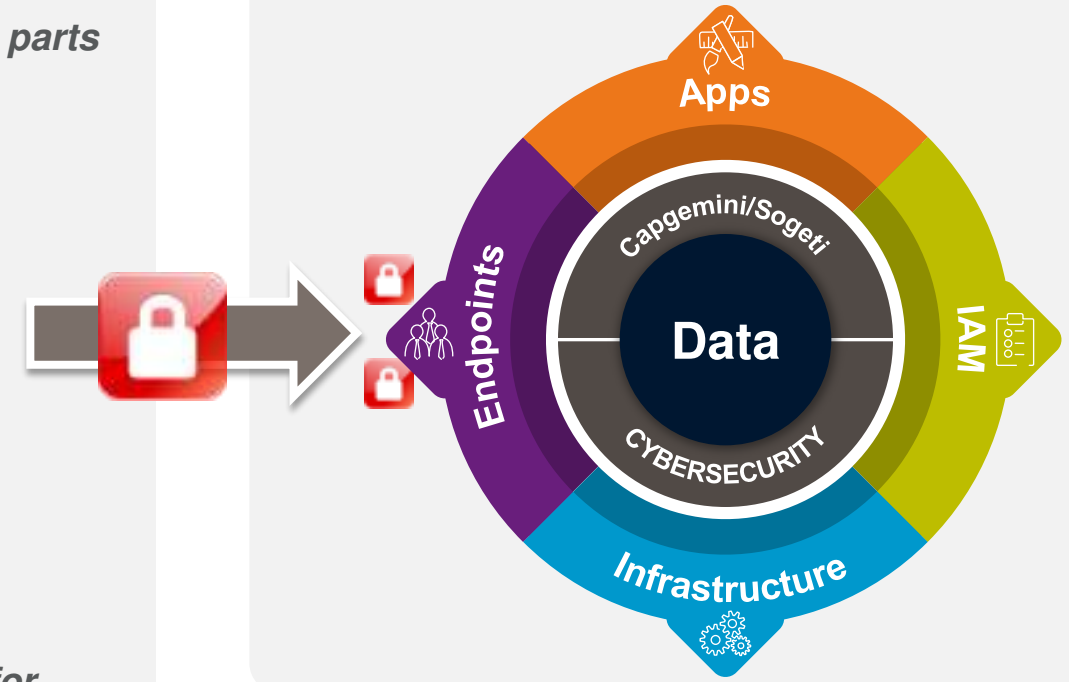
- Gather information
- Scan
- “Hacking” Exploits
- Post exploitation & maintain the access
- Erase traces and evidences

4.3 Security by design : Defense in depth

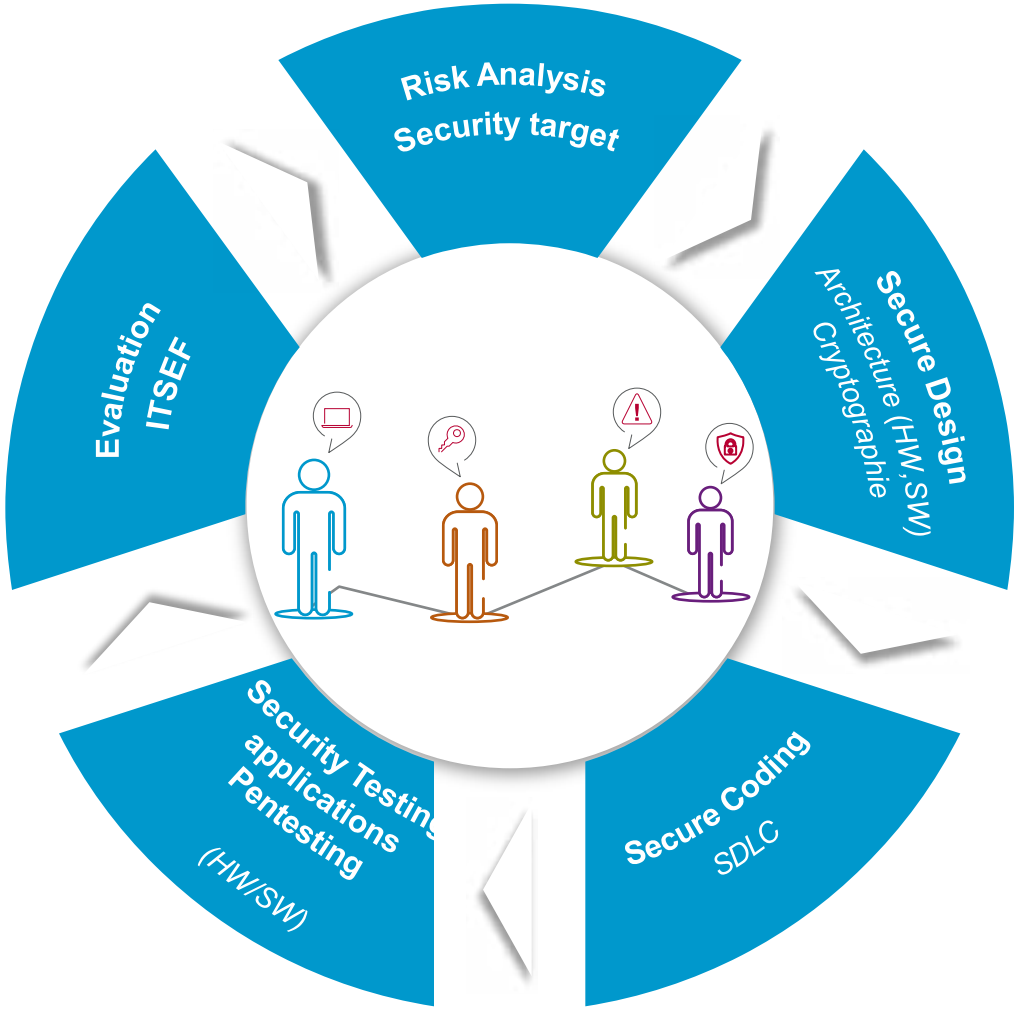
BLOCK a THRETH with an integrated security
Security Architecture – 6 *key principles*

- ***Defense in depth***
- ***Zoning Architecture to insulate sensitive parts***
- ***Define with care Security functions :***
  - ***Access Control*** *(account management, authentication)*
  - *Function separation, Least privilege*
  - ***Control IT ADMINS role, …***
- ***Strengthen products and IT***
- ***Integration of security products***
  anti-malware, NGIPS
  Firewall, email gateway, web gateway, proxies,
  WAF, encryptors, HSM, PAM, IAM,…
- ***Security products and features specific for IOTs (OS, Secure elements, VPN) and industrial systems***

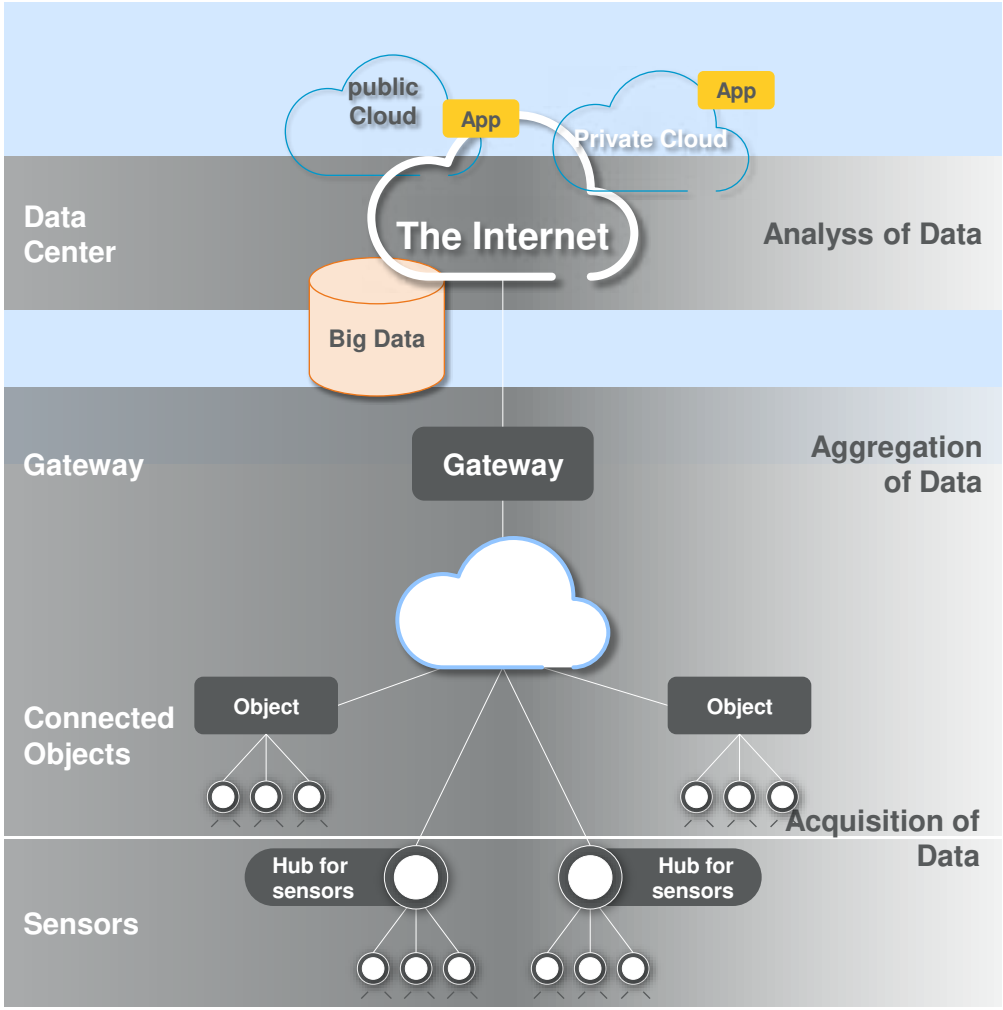
Protection
Integration of systems
Managed Systems



4.3 Security by design, secure build



4.4 Architecture Securing IOTs in IT

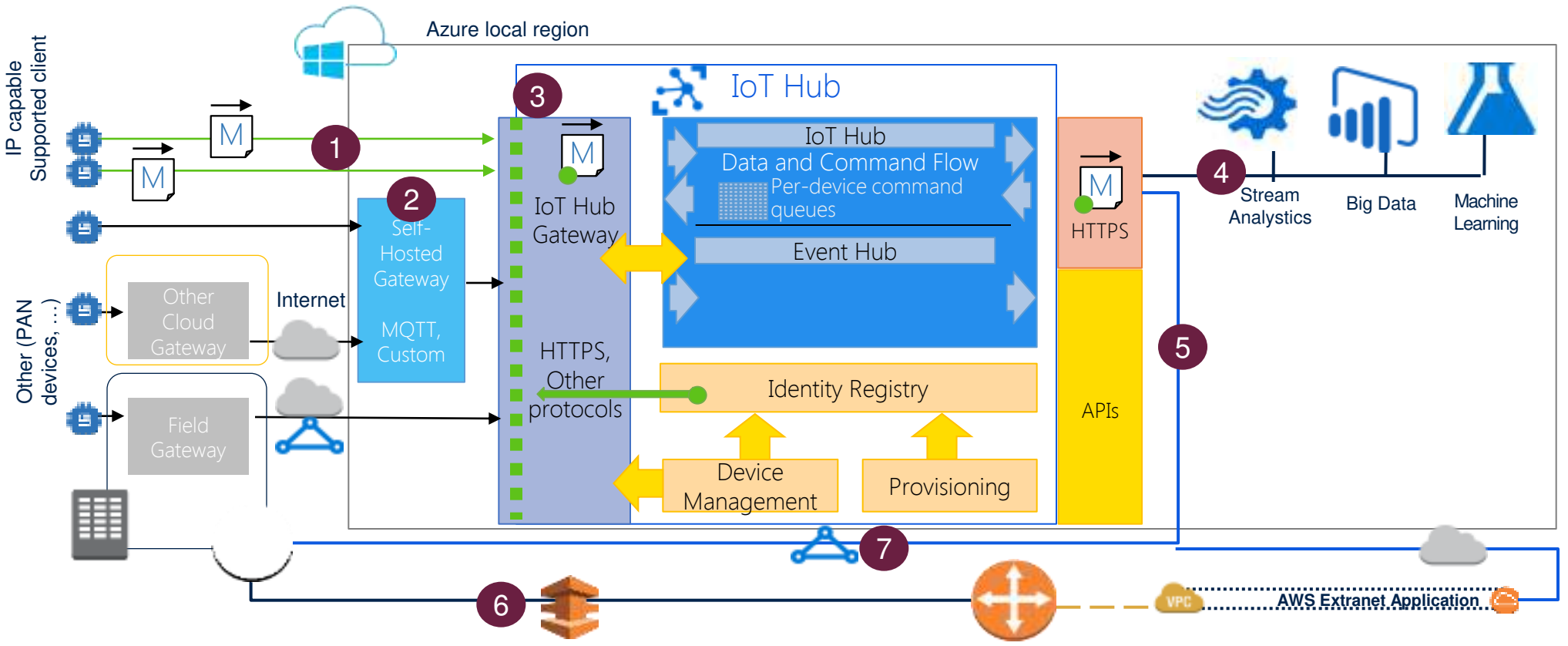


4.3 High-Availability

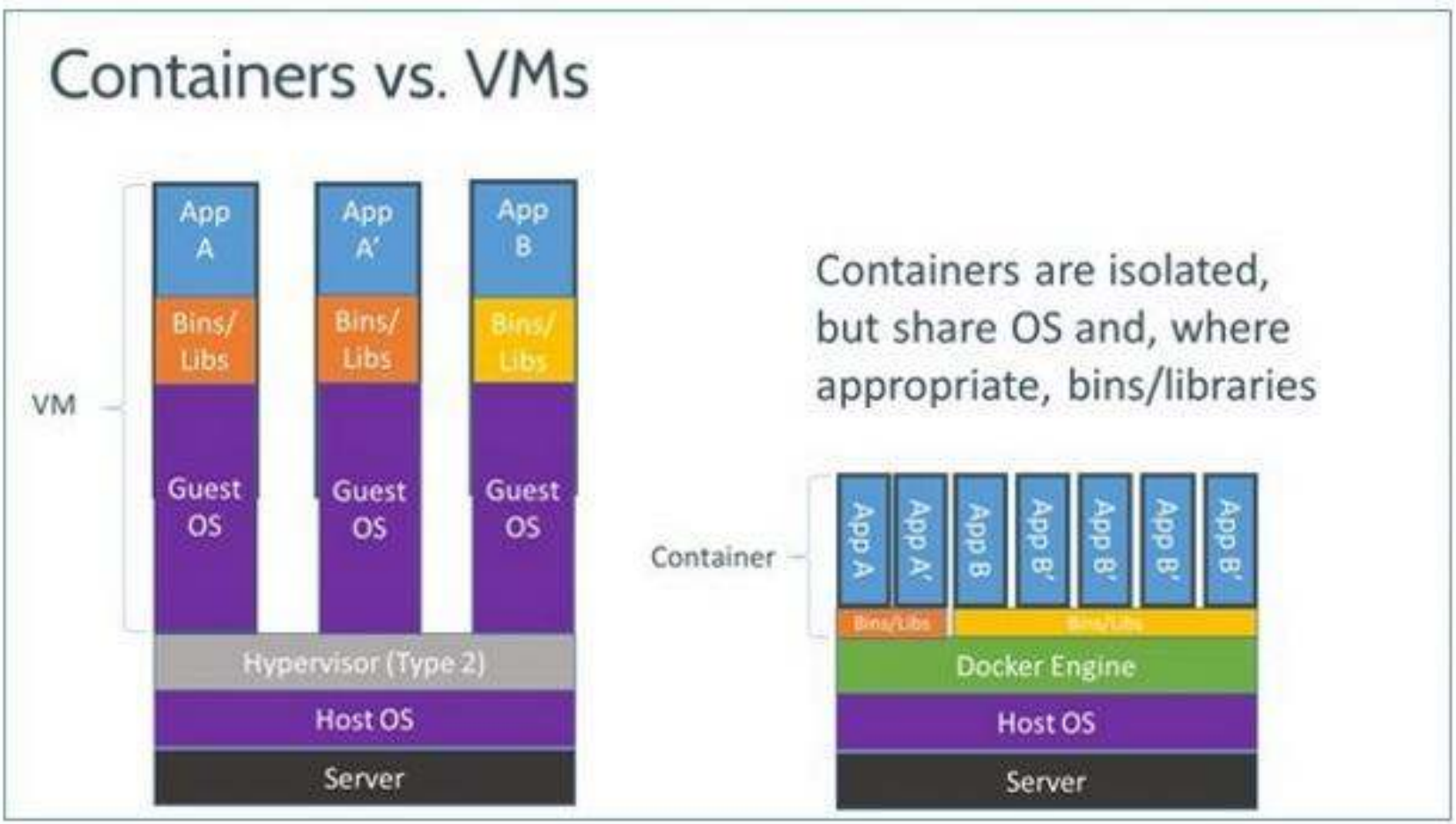
Public IoT platform Integration **with Azure IoT Hub**

Context

This diagram focus is on **acquisition and aggregation layers on public IoT platform** on cloud



4.3 Example of New issues to address



4.3 Secure coding

Your security context

Risk analysis

Methodology
Analysis of existing rules
Definition of a referential
Change management

Security oriented coding rules

Coding rules
C, C++, Java, etc.

Subset of encoding rules to deploy

Providing Tools to the selection rules
-Development of a solution to help manage the profiles selections rules for users

Code review
-Identification of vulnerabilities in the source code
-Analysis Report and recommendations

Developers

Verification tools

Training
-The fundamental security
-Basic Developer training to Secure Coding

4.3 Secure Coding

- **Those rules are organized in 10 principles :**
  - **Never trust the user inputs**
  - **A software must be secured by default**
  - **By default, do not authorized access**
  - **Use the principle of lower privilege**
  - **Always check buffer limits**
  - **Secure the memory management**
  - **Only call trusted functions in signal handler (interruptions)**
  - **Separate the privilege domains**
  - **Be protected against the reverse engineering of the source code**
  - **The execution environment must be secured**

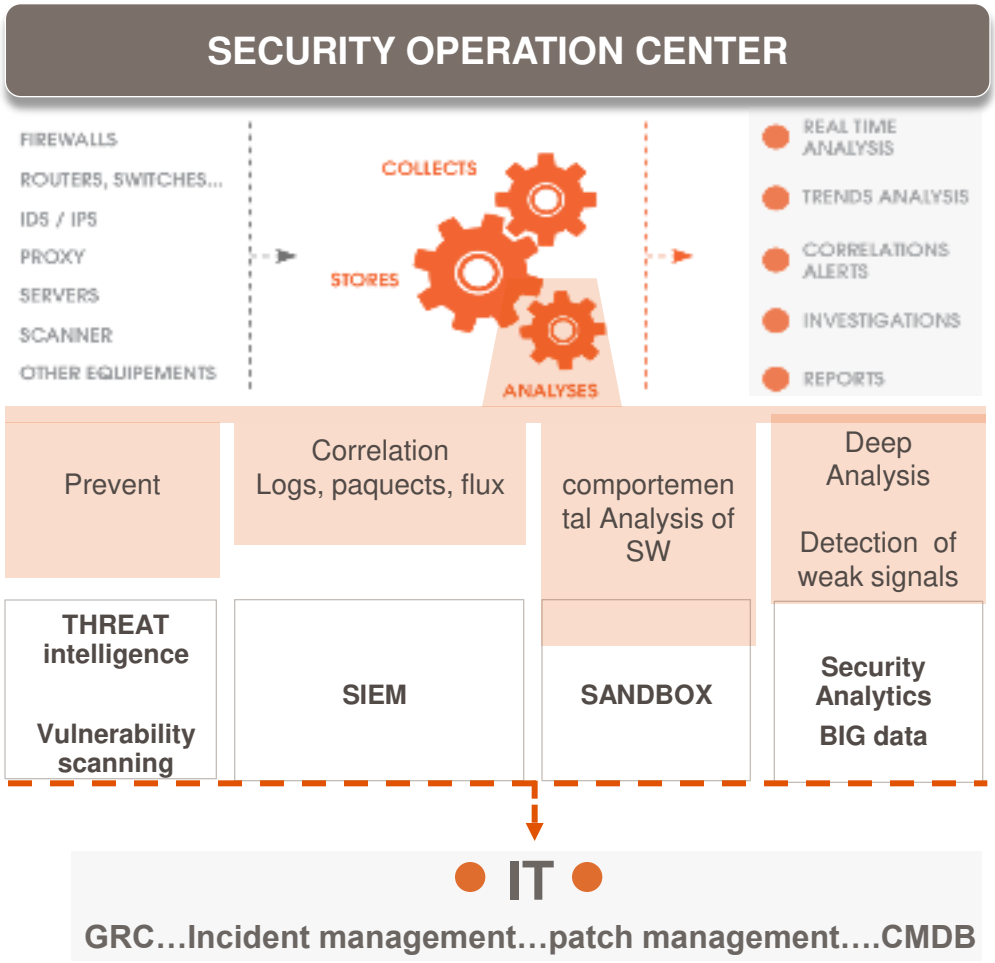
4.3 RUN PHASE: Security Operation Center (SOC)

Supervision of Security
system Integration
Managed Services
SOCaaS

DETECT advances Threats

ACTIV SECURITY

SOCaaS: Security Operation Center as-a Service
SIEM: Security Information and Event Management



About Capgemini and Sogeti

With almost 140,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2013 global revenues of EUR 10.1 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™ and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 2,500 professional employees support you in defining and implementing your cybersecurity strategies. We protect your data, IT and industrial systems, and the Internet of Things (IoT). We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, five security operation centers (SOC) around the world, a licensed Information Technology Security Evaluation Facility, and are a global leader in the field of testing.

www.capgemini.com/cybersecurity
www.sogeti.com/cybersecurity