Source : https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/

Ulrich Seldeslachts ,
Leuven, Dec 8th 2017

ConnectedFactories

Cluster Management Excellence

ACDC

TAKEDOWN Identify . Prevent . Respond

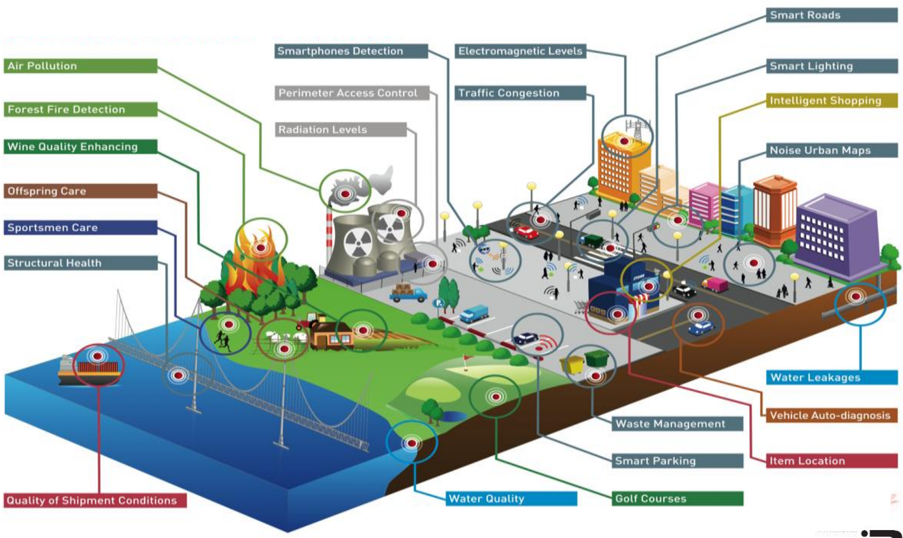
European Commission

LSEC LEADERS IN SECURITY

3IF.be

Source : https://blog.perfectcloud.io/internet-of-things-identity-management/

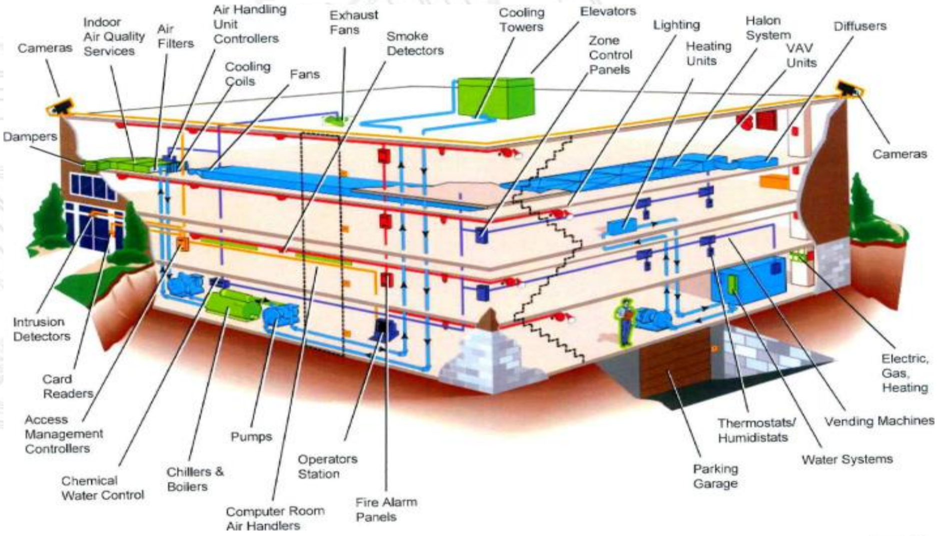
… towards a Smart World



Source: Libelium

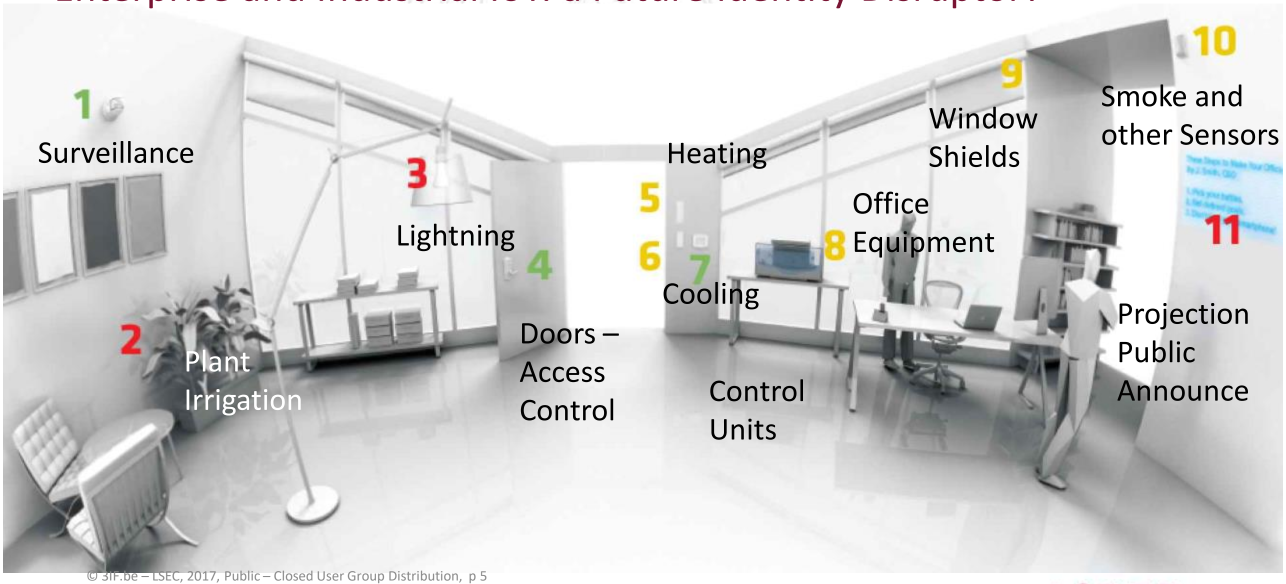
3IF.be LSEC LEADERS IN SECURITY

… a connected business environment

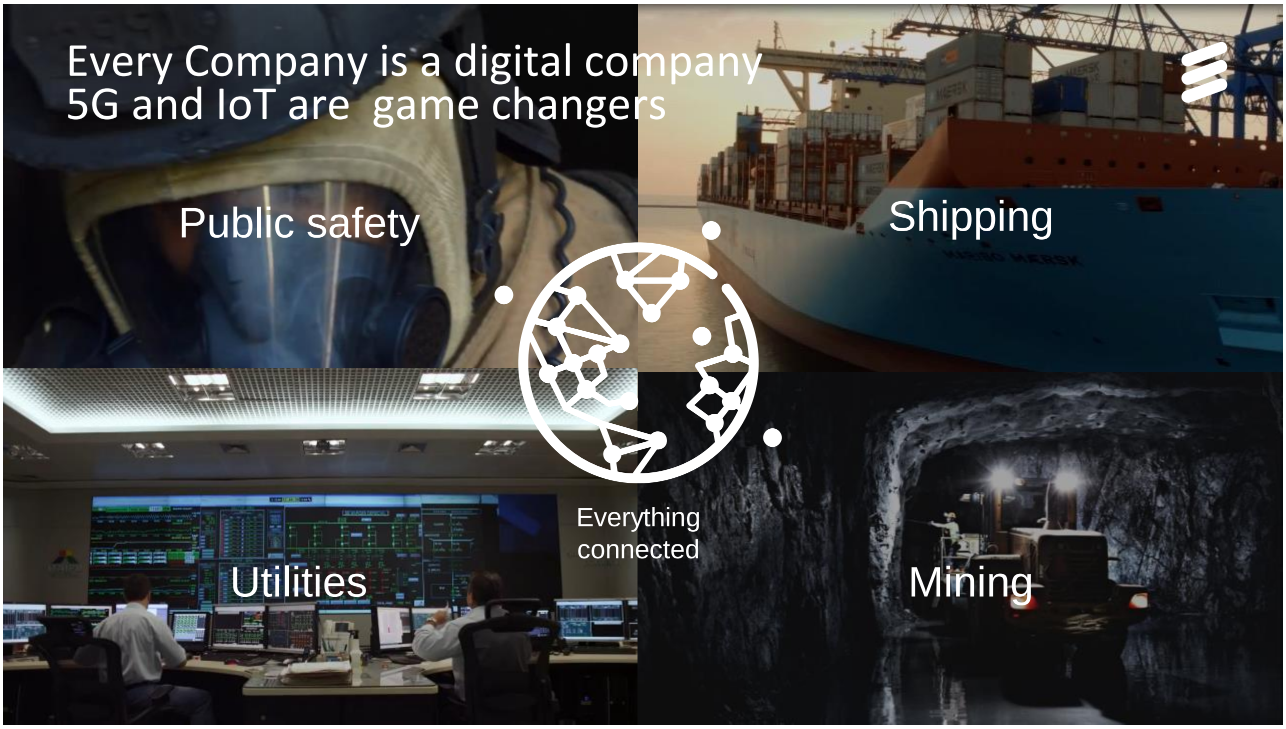


Source: BI Intelligence, 2015

Enterprise and Industrial IoT: a Future Identity Disruptor?



Every Company is a digital company
5G and IoT are game changers



Industrie 4.0, Industrial Internet, Smart Manufacturing indicate the level of Digitalisation of Manufacturing

Legacy and Smarter Devices are being connected to Drive Operational Efficiency

Smarter production will allow Mass Customization

Source: LSEC – 3IF.be, Siemens, 2016

Connectivity & sensing

Massive influx of data & connectivity of systems

Advanced analytics

Use of greater portion of **data via Advanced** Analytics and **machine learning**

Robotics & Automation

Automation (or semi-automation) of major portions of value chain

Process digitization

Mobile tools for **field-force** and **manage-ment support**

90%

Data in the world today has been created in the last two years

10^{15}

More computer operations per second than since the 1960s

50%

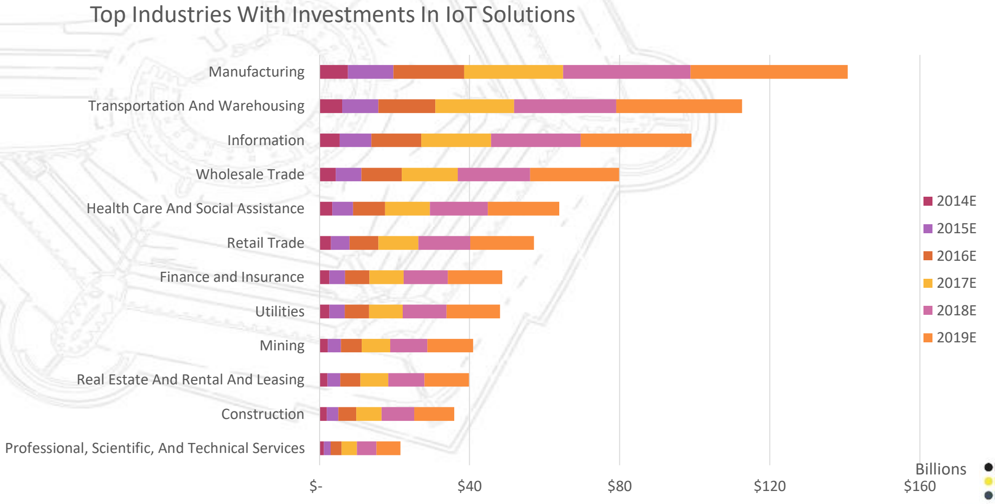
Reduction in cost of robots since 1990 vs 80% increase in US labour costs

250k x

More RAM in iPhone 5 than in the Apollo 11 computer

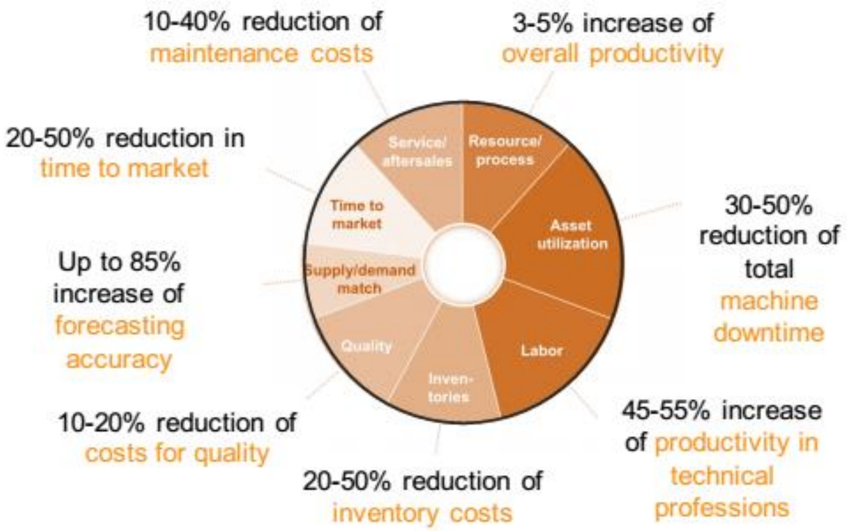
Source: McKinsey & Co, 2017

IoT… manufacturing to lead, logistics early adopter



Source: BI Intelligence, 2015

The potential of I4.0



10-40% reduction of maintenance costs

3-5% increase of overall productivity

20-50% reduction in time to market

30-50% reduction of total machine downtime

Up to 85% increase of forecasting accuracy

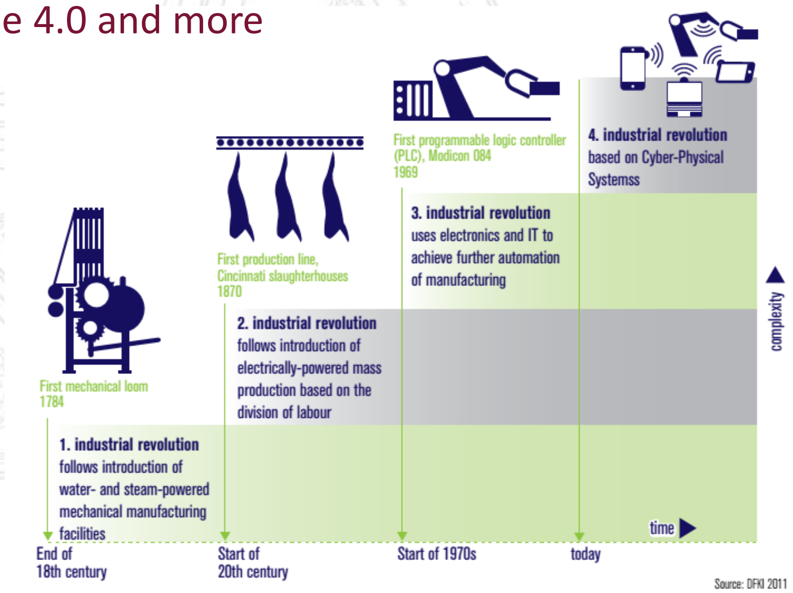
10-20% reduction of costs for quality

20-50% reduction of inventory costs

45-55% increase of productivity in technical professions

Source : German Innovation Center for I4.0, 2017

Industrie 4.0 and more



First mechanical loom 1784

1. industrial revolution follows introduction of water- and steam-powered mechanical manufacturing facilities

First production line, Cincinnati slaughterhouses 1870

2. industrial revolution follows introduction of electrically-powered mass production based on the division of labour

First programmable logic controller (PLC), Modicon 084 1969

3. industrial revolution uses electronics and IT to achieve further automation of manufacturing

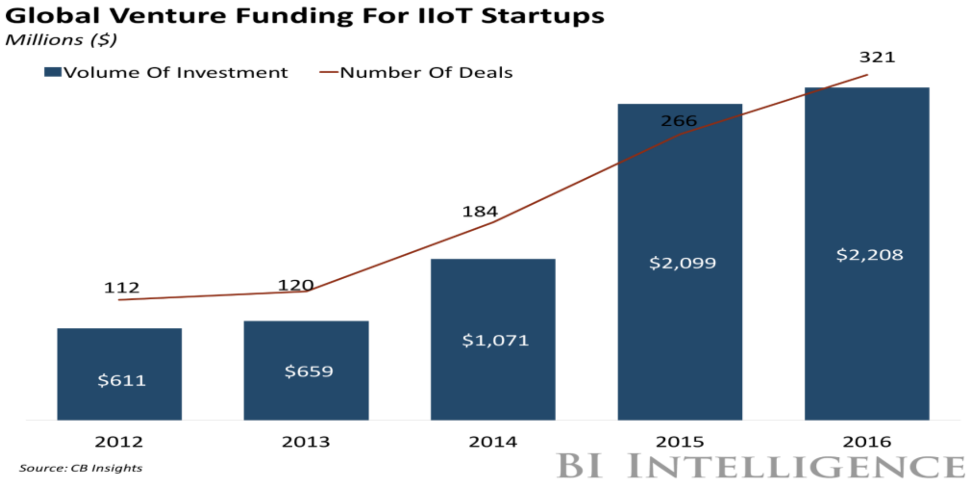
4. industrial revolution based on Cyber-Physical Systemss

Source: DFKI 2011

Source : Plattform Industrie 4.0, 2013

The Fourth Industrial Revolution
Klaus Schwab
Industry 4.0
The Industrial Internet of Things
Alasdair Gilchrist
Apress
THE INDUSTRIES OF THE FUTURE
ALEC ROSS

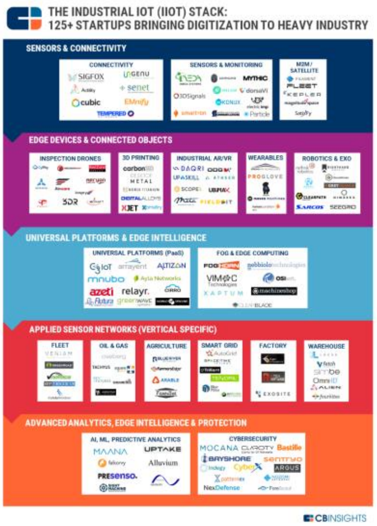
The next big thing?



Source: CB Insights

Source: BI Intelligence, 2017

The next big thing for Electronics Designers & Manufacturers


THE INDUSTRIAL IOT (IIOT) STACK:
125+ STARTUPS BRINGING DIGITIZATION TO HEAVY INDUSTRY
SENSORS & CONNECTIVITY
CONNECTIVITY
SENSORS & MONITORING
M2M / SATELLITE
EDGE DEVICES & CONNECTED OBJECTS
INSPECTION DRONES
3D PRINTING
INDUSTRIAL AR/VR
WEARABLES
ROBOTICS & EXO
UNIVERSAL PLATFORMS & EDGE INTELLIGENCE
UNIVERSAL PLATFORMS (PaaS)
FOG & EDGE COMPUTING
APPLIED SENSOR NETWORKS (VERTICAL SPECIFIC)
FLEET
OIL & GAS
AGRICULTURE
SMART GRID
FACTORY
WAREHOUSE
ADVANCED ANALYTICS, EDGE INTELLIGENCE & PROTECTION
AI, ML, PREDICTIVE ANALYTICS
CYBERSECURITY
CBINSIGHTS

1. **Sensors & Connectivity**
    1. **Connectivity**
    2. **Sensors & Monitoring**
    3. **M2M / Satellite**
2. **Edge Devices & Connected Objects**
    1. **Inspection Drones**
    2. **3D Printing**
    3. **Industrial AR/VR**
    4. **Wearables**
    5. **Robotics & Exo**
3. **Universal Platforms & Edge Intelligence**
    1. **Universal Platforms**
    2. **Fog & Edge Computing**
4. **Applied Sensor Networks**
    4. **Fleet**
    5. **Oil & Gas**
    6. **Agriculture**
    7. **Smart Grid**
    8. **Factory**
    9. **Warehouse**
5. **Advanced Analytics, Edge Intelli**
    1. **AI, ML, Predictive Analytics**
    2. **Cybersecurity**

Source: CB Insights 2017

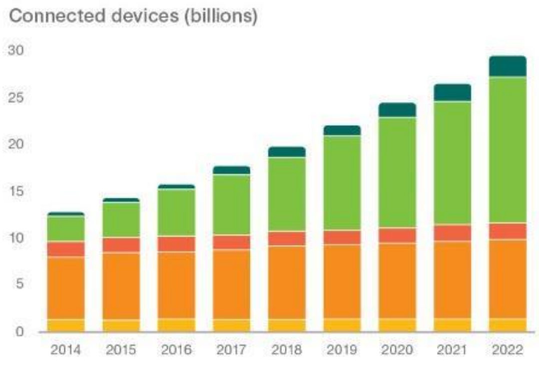
The industrial internet is here to stay. 50B devices connecting by 2020

Security Incidents are increasing in frequency, sophistication and impact

The only way to address security is an automated end-to-end approach and highly skilled professionals.

Source: Wurldtech 2016

29 billion devices – 29 billion sources of potential threat

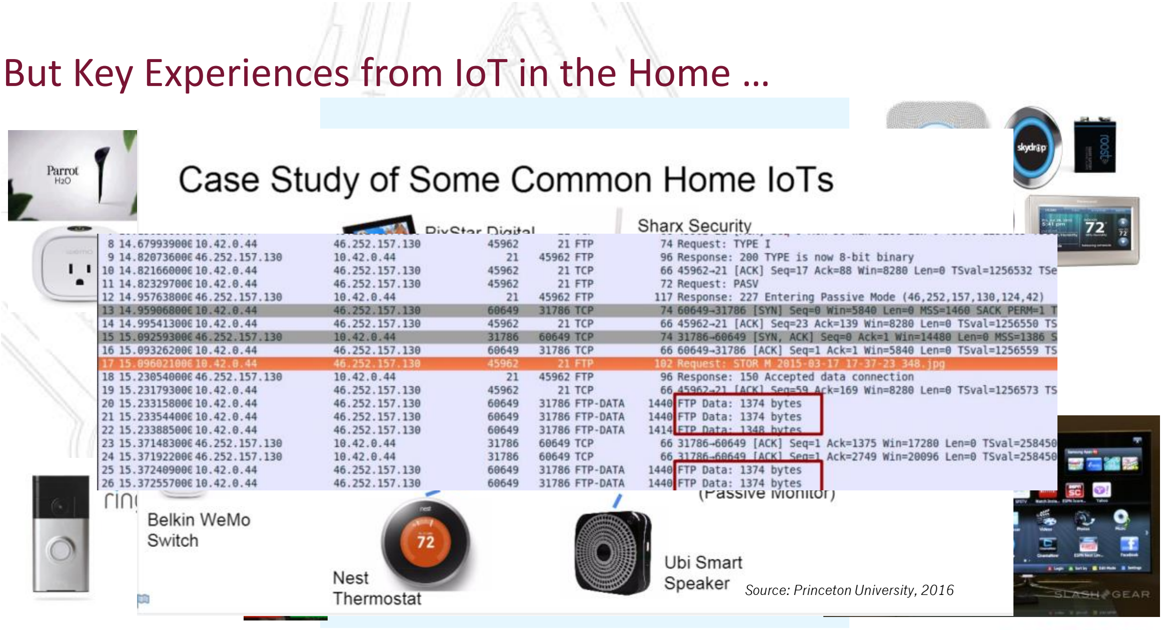


	2016	2022	CAGR
Wide-area IoT	0.4	2.1	30%
Short-range IoT	5.2	16	20%
PC/laptop/tablet	1.6	1.7	0%
Mobile phones	7.3	8.6	3%
Fixed phones	1.4	1.3	0%
	16 billion	29 billion	10%

Source: Ericsson Mobility Report, Nov 2016

Commercial in confidence | © Ericsson AB 2016 | 2016-12-30 | Page 17

But Key Experiences from IoT in the Home …



Case Study of Some Common Home IoTs

PixStar Digital

Sharx Security

```
 8 14.67993900€ 10.42.0.44       46.252.157.130   45962    21 FTP       74 Request: TYPE I
 9 14.82073600€ 46.252.157.130   10.42.0.44          21 45962 FTP       96 Response: 200 TYPE is now 8-bit binary
10 14.82166000€ 10.42.0.44       46.252.157.130   45962    21 TCP       66 45962→21 [ACK] Seq=17 Ack=88 Win=8280 Len=0 TSval=1256532 TSe
11 14.82329700€ 10.42.0.44       46.252.157.130   45962    21 FTP       72 Request: PASV
12 14.95763800€ 46.252.157.130   10.42.0.44          21 45962 FTP      117 Response: 227 Entering Passive Mode (46,252,157,130,124,42)
13 14.95906800€ 10.42.0.44       46.252.157.130   60649 31786 TCP       74 60649→31786 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 T
14 14.99541300€ 10.42.0.44       46.252.157.130   45962    21 TCP       66 45962→21 [ACK] Seq=23 Ack=139 Win=8280 Len=0 TSval=1256550 TS
15 15.09259300€ 46.252.157.130   10.42.0.44       31786 60649 TCP       74 31786→60649 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 S
16 15.09326200€ 10.42.0.44       46.252.157.130   60649 31786 TCP       66 60649→31786 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=1256559 TS
17 15.09602100€ 10.42.0.44       46.252.157.130   45962    21 FTP      102 Request: STOR M 2015-03-17 17-37-23 348.jpg
18 15.23054000€ 46.252.157.130   10.42.0.44          21 45962 FTP       96 Response: 150 Accepted data connection
19 15.23179300€ 10.42.0.44       46.252.157.130   45962    21 TCP       66 45962→21 [ACK] Seq=59 Ack=169 Win=8280 Len=0 TSval=1256573 TS
20 15.23315800€ 10.42.0.44       46.252.157.130   60649 31786 FTP-DATA 1440 FTP Data: 1374 bytes
21 15.23354400€ 10.42.0.44       46.252.157.130   60649 31786 FTP-DATA 1440 FTP Data: 1374 bytes
22 15.23388500€ 10.42.0.44       46.252.157.130   60649 31786 FTP-DATA 1414 FTP Data: 1348 bytes
23 15.37148300€ 46.252.157.130   10.42.0.44       31786 60649 TCP       66 31786→60649 [ACK] Seq=1 Ack=1375 Win=17280 Len=0 TSval=258450
24 15.37192200€ 46.252.157.130   10.42.0.44       31786 60649 TCP       66 31786→60649 [ACK] Seq=1 Ack=2749 Win=20096 Len=0 TSval=258450
25 15.37240900€ 10.42.0.44       46.252.157.130   60649 31786 FTP-DATA 1440 FTP Data: 1374 bytes
26 15.37255700€ 10.42.0.44       46.252.157.130   60649 31786 FTP-DATA 1440 FTP Data: 1374 bytes
```

(Passive Monitor)

Belkin WeMo Switch

Nest Thermostat

Ubi Smart Speaker

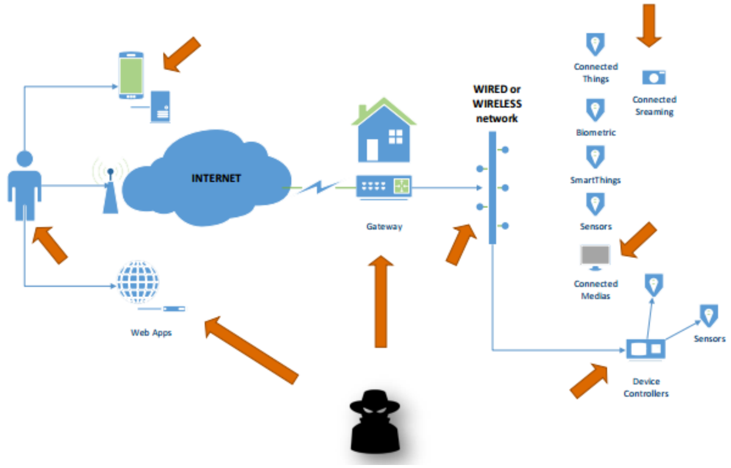
Source: Princeton University, 2016

© Leaders in Security – LSEC – 3IF.be, 2017, Public – Closed User Group Distribution, p 18

Source: BI Intelligence, 2015

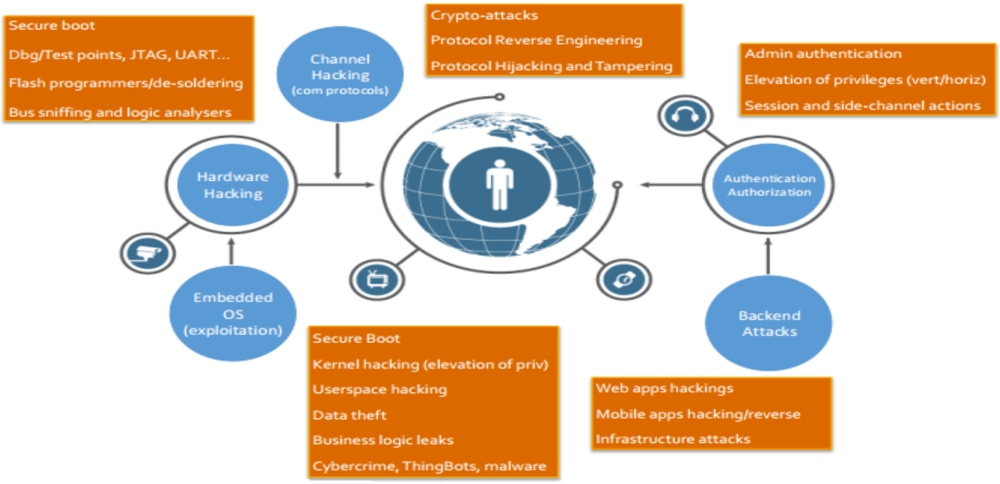
… learn that IoT Devices are a Cyber Target!

IoT design, attacks in a nutshell



Source: LSEC IoT Security 2015, PWC

Top 5 IoT attack vectors



Secure boot
Dbg/Test points, JTAG, UART…
Flash programmers/de-soldering
Bus sniffing and logic analysers

Channel Hacking (com protocols)

Crypto-attacks
Protocol Reverse Engineering
Protocol Hijacking and Tampering

Admin authentication
Elevation of privileges (vert/horiz)
Session and side-channel actions

Hardware Hacking

Authentication Authorization

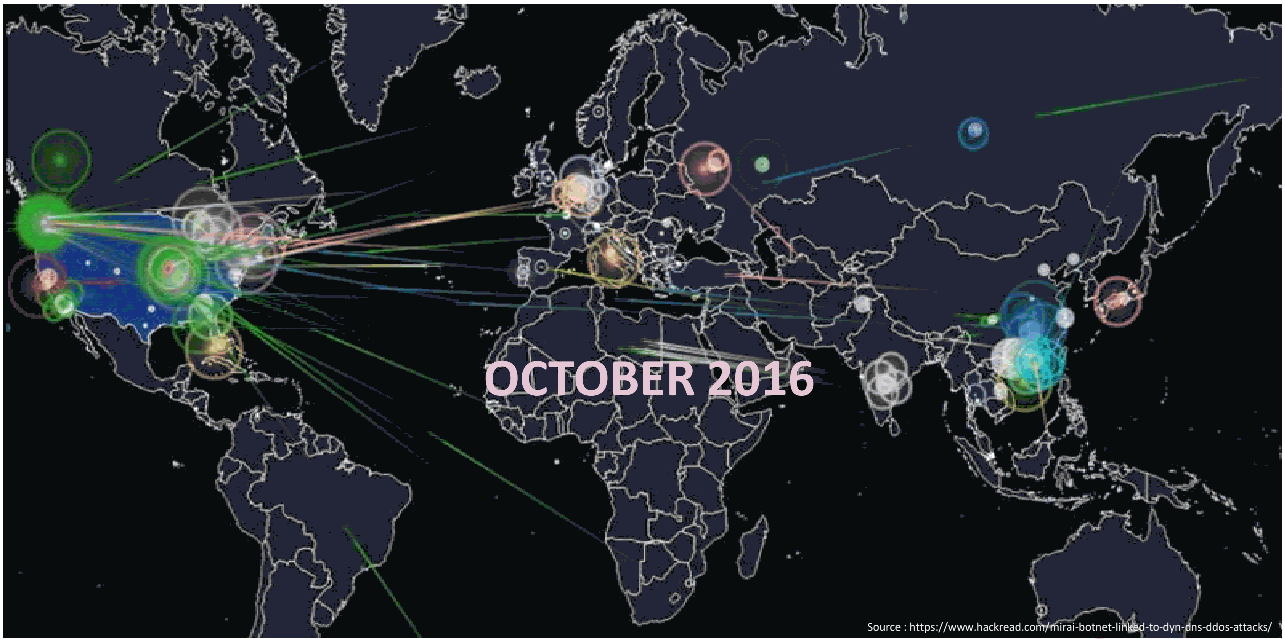
Embedded OS (exploitation)

Backend Attacks

Secure Boot
Kernel hacking (elevation of priv)
Userspace hacking
Data theft
Business logic leaks
Cybercrime, ThingBots, malware

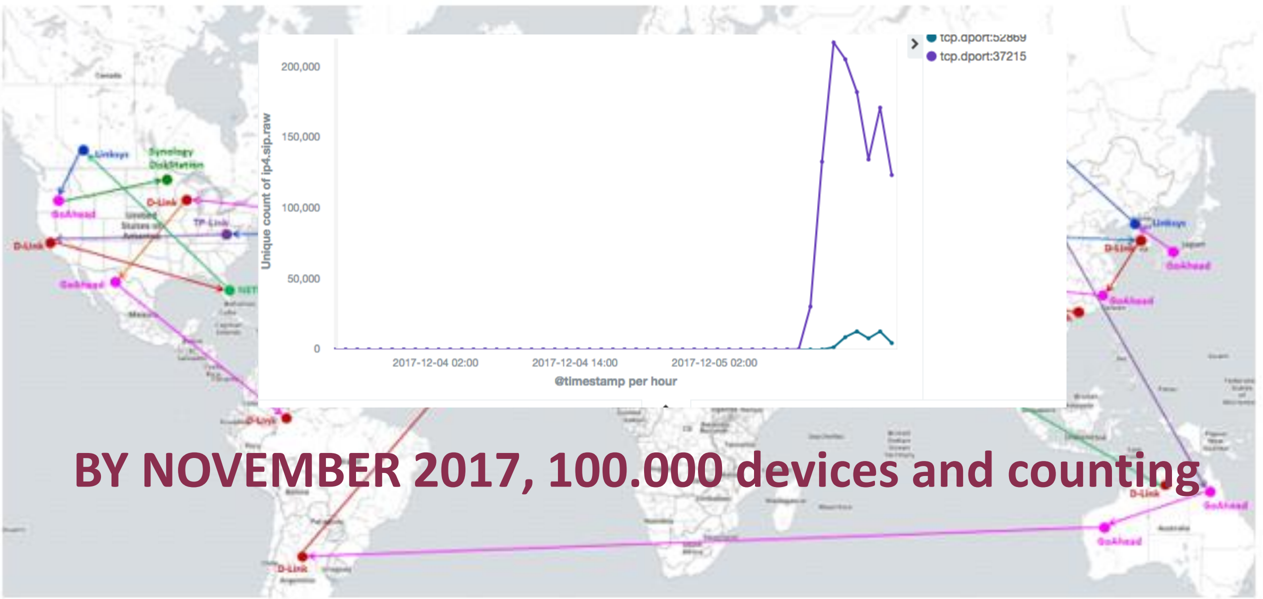
Web apps hackings
Mobile apps hacking/reverse
Infrastructure attacks

Source : LSEC IoT Security, 2015, PWC



OCTOBER 2016

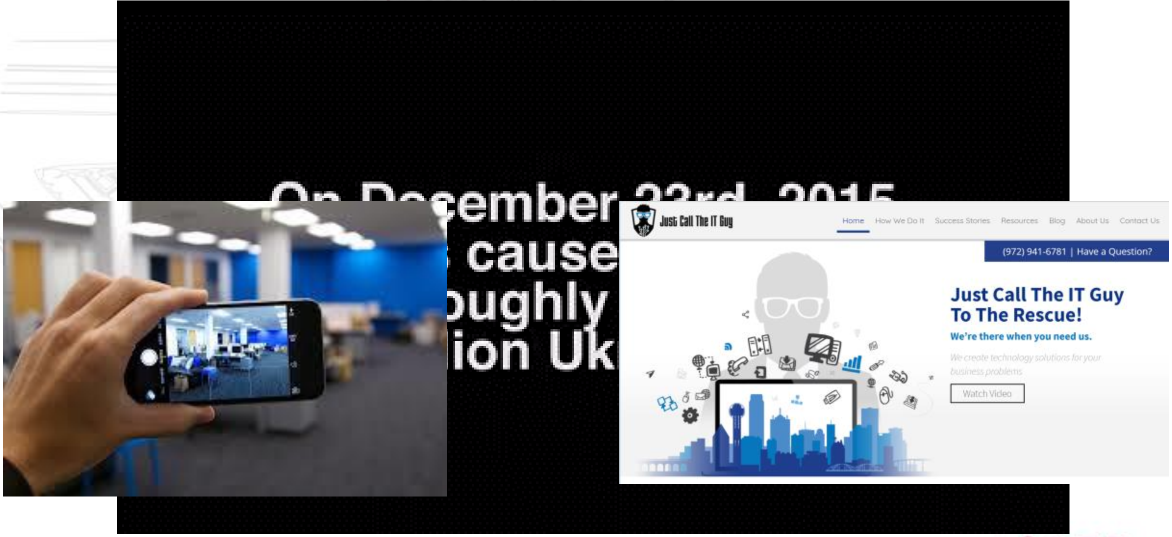
Source : https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/



BY NOVEMBER 2017, 100.000 devices and counting

Source : Checkpoint, Netlab365

Next : From Hacking to Terrorism



Just Call The IT Guy To The Rescue!

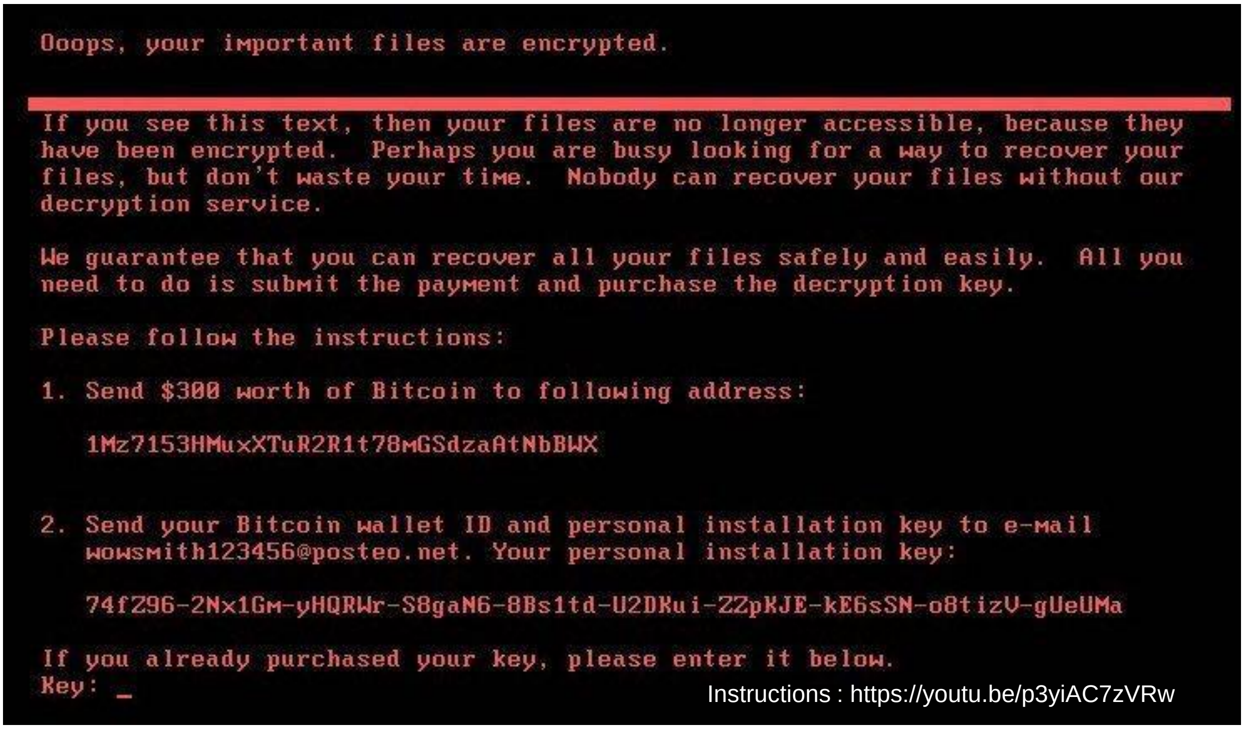
We're there when you need us.

We create technology solutions for your business problems

Source : https://www.wired.com/story/russian-hackers-attack-ukraine/

Impact on National Security

Source: Wired, AFP



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Instructions : https://youtu.be/p3yiAC7zVRw

The Basics : 1 – Ransomware – ICS (In)Security & Easy Target

NBU: Third of Ukrainian banks hit by last week's cyber attack

By Interfax-Ukraine. Published July 6 at 9:19 pm

The NotPetya ransomware running

http://cert-mu

Small cyber attack hits Russia and Ukraine

October 24, 2017

A statement issued by Group-IB said a cyber attack on October 23, 2017, appeared to have its origins in Russia and had also affected some corporate sites in Turkey and Germany

© Leaders in Security – LSEC – 3IF.be, 2017, Public – Closed User Group Distribution, p 26

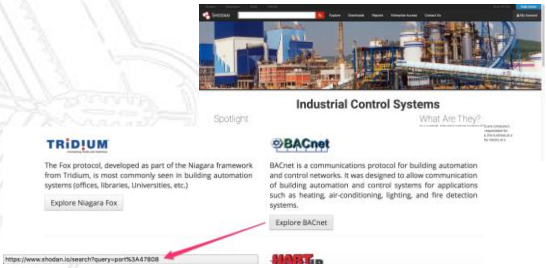
Source: AFP, Hackernews, Evraz, Guardian

The Basics : 2 – Shodan Public ICS Results

- **Query Shodan**
  - "Industrial Control Systems"
    - Predefined ports, strings
  - + some popular strings/vendors

- **api.search**(expr);
  - Per result api.host(ip_str, history=False)
    - Hostname, domain, open ports
    - SQLite **Database**
    - Only if combination of host+port+transport isn't already there;

- Extract **product and device information**;
  - Shodan info (device_type, product_name, vendor_id, shodan_module)
  - Simple banner parsing (also from Shodan)
    - 1° Product name ; 2° HTTP Banner ; 3° First strings in Shodan data object



Industrial Control Systems

Spotlight

What Are They?

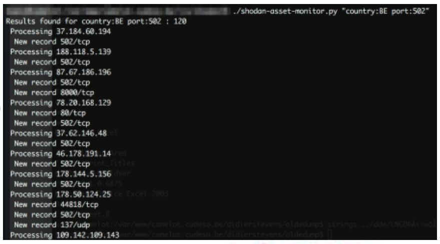
TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

https://www.shodan.io/search?query=port%3A47808



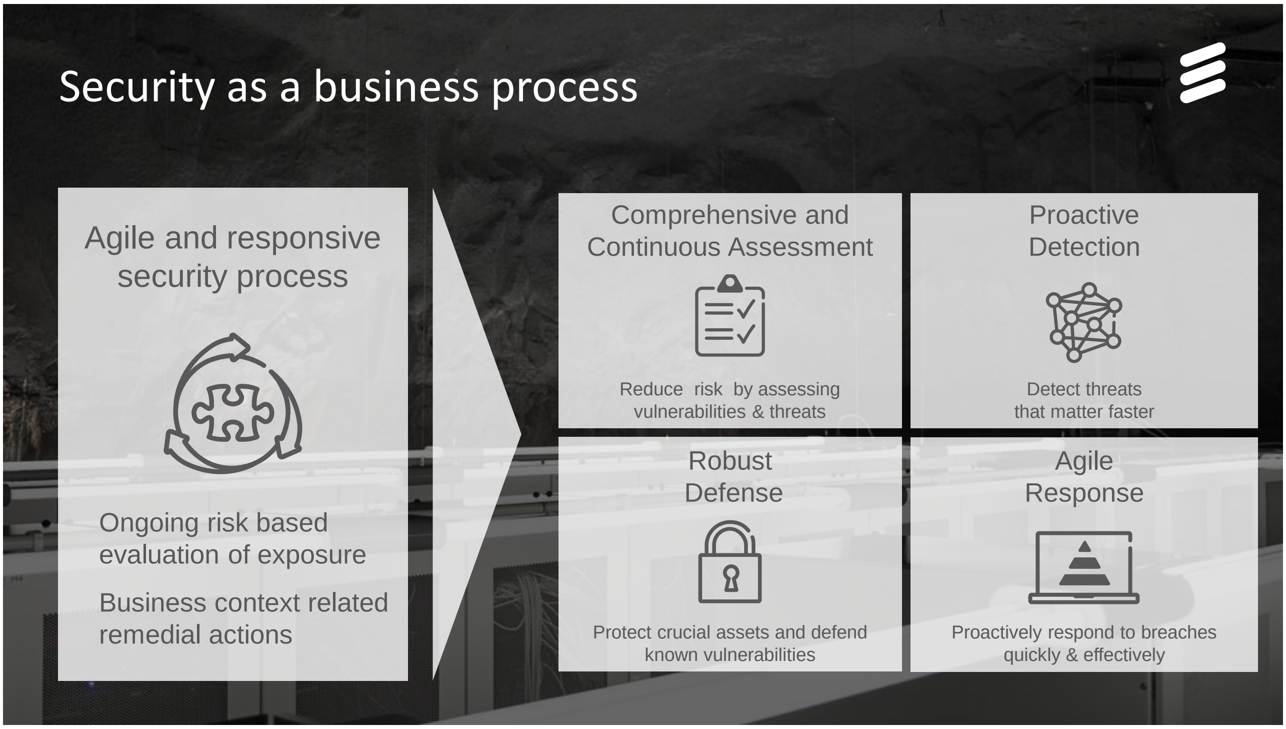
```
[redacted] ./shodan-asset-monitor.py "country:BE port:502"
Results found for country:BE port:502 : 120
 Processing 37.184.60.194
  New record 502/tcp
 Processing 188.118.5.139
  New record 502/tcp
 Processing 87.67.186.196
  New record 502/tcp
  New record 8000/tcp
 Processing 78.20.168.129
  New record 80/tcp
  New record 502/tcp
 Processing 37.62.146.48
  New record 502/tcp
 Processing 46.178.191.14
  New record 502/tcp
 Processing 178.144.5.156
  New record 502/tcp
 Processing 178.50.124.25
  New record 44818/tcp
  New record 502/tcp
  New record 137/udp
 Processing 109.142.109.143
```

Source: Cudeso, Koen Van Impe, 2017

Digital Factories and Industrial Industrial Internet require Smart and Secure Devices

Collecting Data and Providing Insights into Factory Operations and Security Incidents AI Driven Advanced Analytics

Machine Learning and Highly Skilled Cyber Security Experts drive Automated Mitigation and Response



Security as a business process

Agile and responsive security process

Ongoing risk based evaluation of exposure

Business context related remedial actions

Comprehensive and Continuous Assessment

Reduce risk by assessing vulnerabilities & threats

Proactive Detection

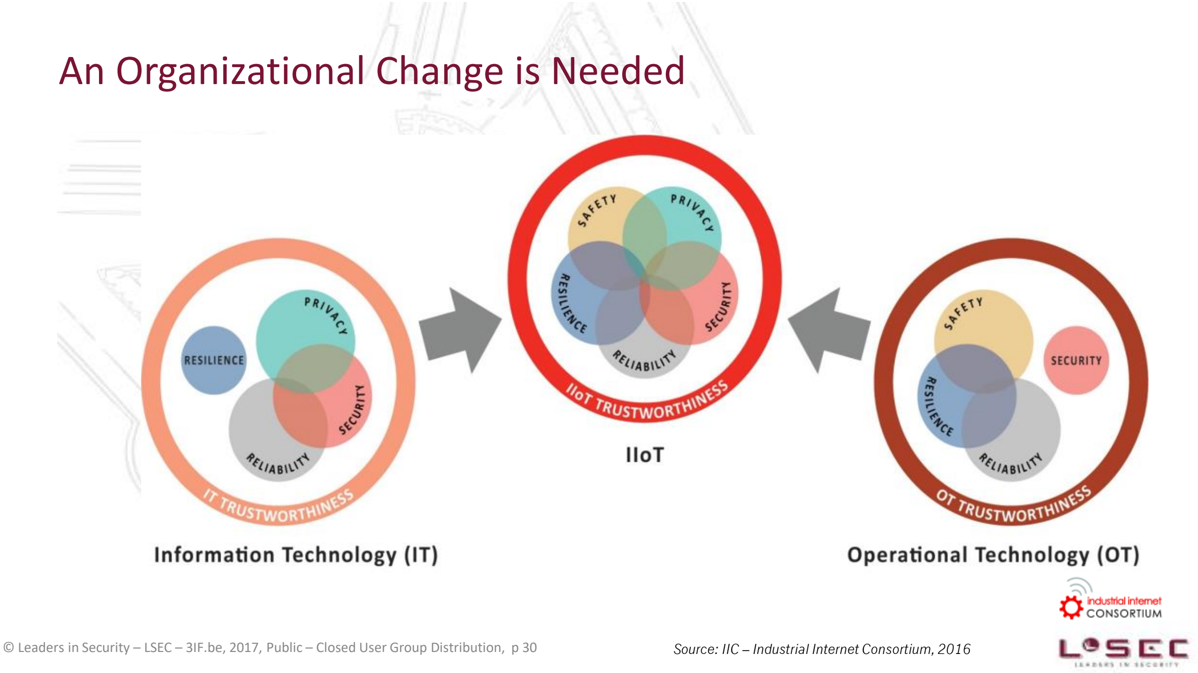
Detect threats that matter faster

Robust Defense

Protect crucial assets and defend known vulnerabilities

Agile Response

Proactively respond to breaches quickly & effectively



An Organizational Change is Needed

Information Technology (IT)

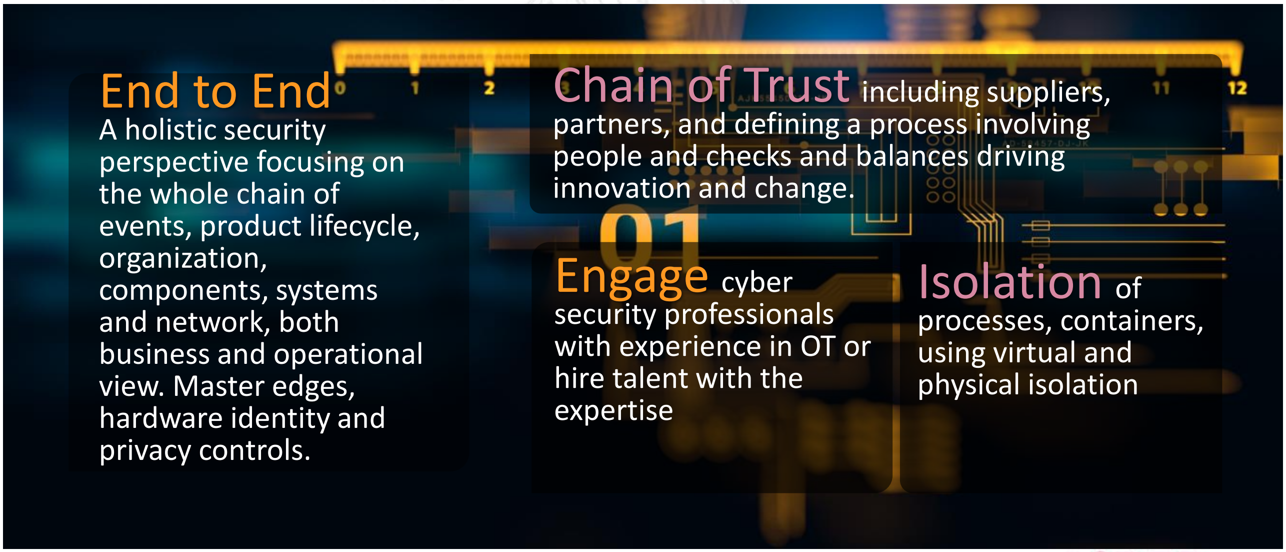
IIoT

Operational Technology (OT)

© Leaders in Security – LSEC – 3IF.be, 2017, Public – Closed User Group Distribution, p 30

Source: IIC – Industrial Internet Consortium, 2016

Smart & Secure Devices : Opportunities & Challenges



End to End
A holistic security perspective focusing on the whole chain of events, product lifecycle, organization, components, systems and network, both business and operational view. Master edges, hardware identity and privacy controls.

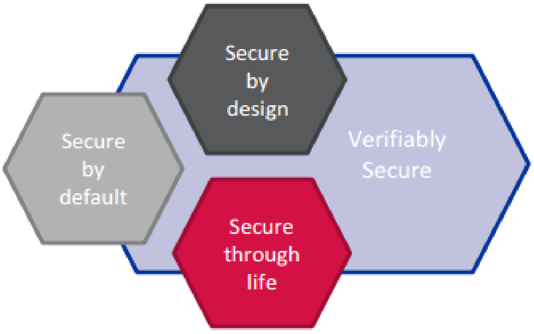
Chain of Trust including suppliers, partners, and defining a process involving people and checks and balances driving innovation and change.

Engage cyber security professionals with experience in OT or hire talent with the expertise

Isolation of processes, containers, using virtual and physical isolation

Source : LSEC, 3IF.be, IIC, GE Wurldtech, 2016

Digital Platforms – Cybersecurity - highlights

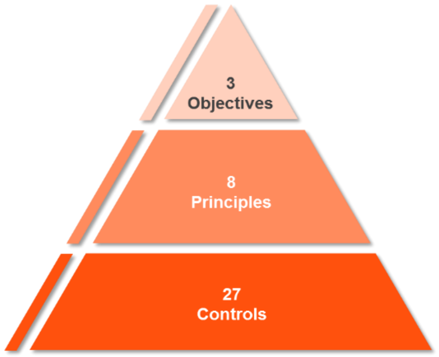


Baseline Security Recommendations for IoT
in the context of Critical Information Infrastructures

ENISA, November 2017

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 723777)

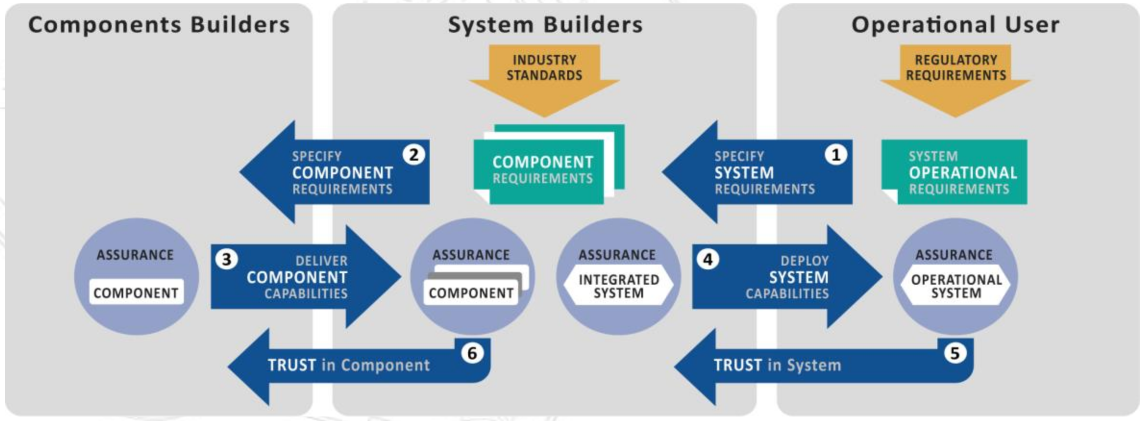
Recommendation - Cybersecurity – Control Framework



1) **secure your environment**
   a. Restrict Internet Access
   b. Segregate critical systems from general IT environment
   c. Reduce attack surface and vulnerabilities
   d. Physically secure the environment
2) **know and limit access**
   a. Prevent compromise of credentials
   b. Manage identities and segregate privileges
3) **detect and respond**
   a. Detect anomalous activity to system or transaction records
   b. Plan for incident response and information sharing

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 723777)

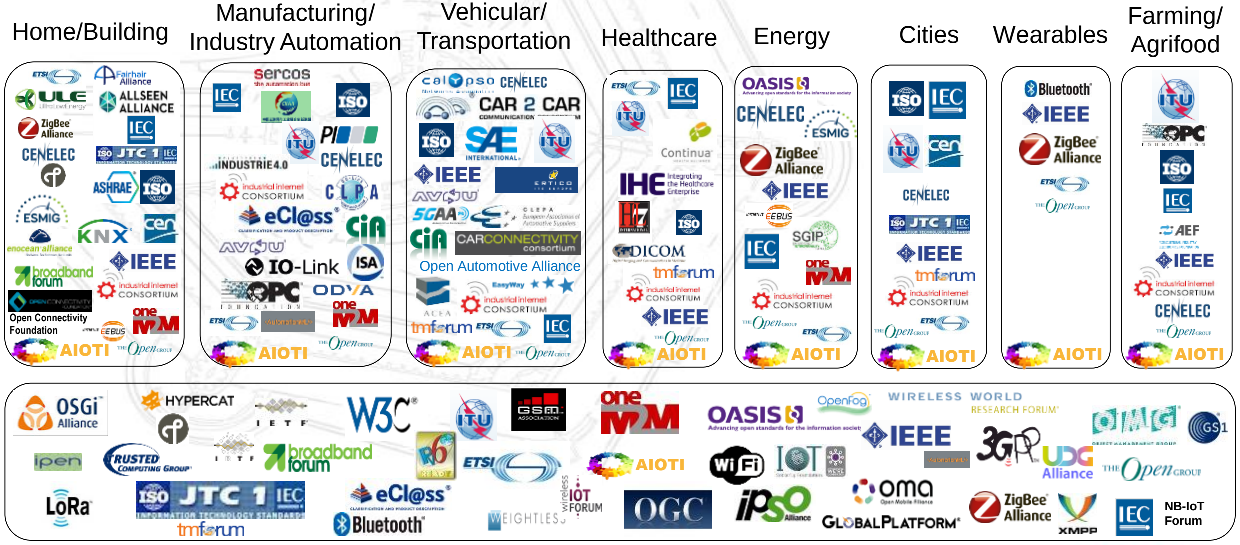
IIC Security Framework : security reference model


Components Builders
System Builders
Operational User
INDUSTRY STANDARDS
REGULATORY REQUIREMENTS
SPECIFY COMPONENT REQUIREMENTS 2
COMPONENT REQUIREMENTS
SPECIFY SYSTEM REQUIREMENTS 1
SYSTEM OPERATIONAL REQUIREMENTS
ASSURANCE COMPONENT
3 DELIVER COMPONENT CAPABILITIES
ASSURANCE COMPONENT
ASSURANCE INTEGRATED SYSTEM
4 DEPLOY SYSTEM CAPABILITIES
ASSURANCE OPERATIONAL SYSTEM
TRUST in Component 6
TRUST in System 5

Trust flows down from the owner/operator to all parts of the IIoT system, but trust must be enabled from the bottom up.

Source: IIC – Industrial Internet Consortium, 2016

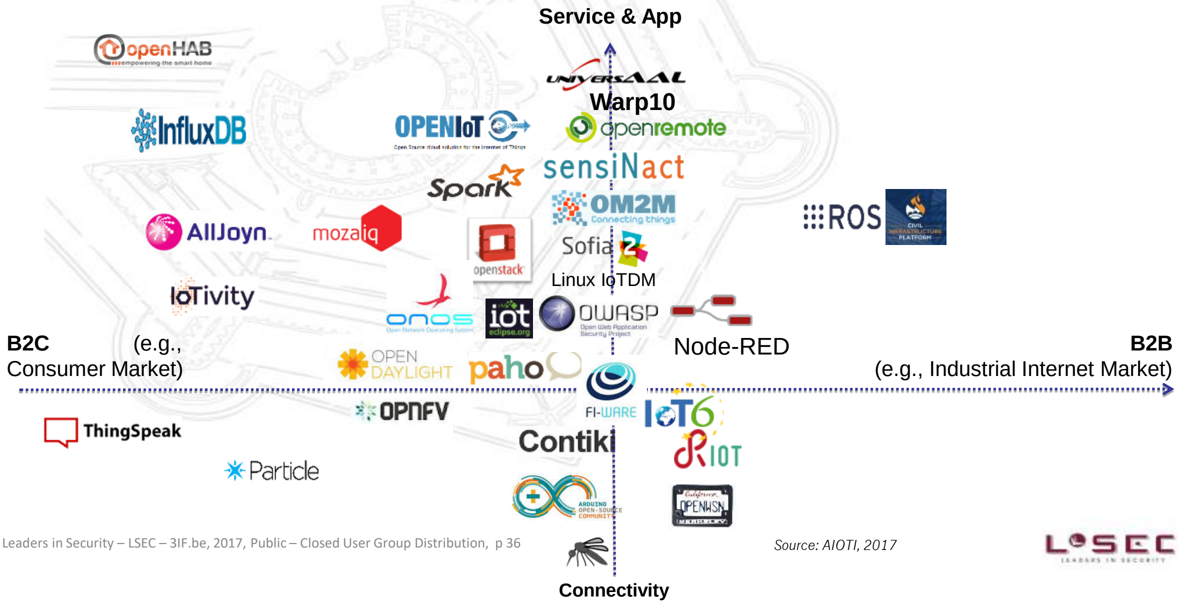
Or Go to Standards – but there's a couple of them



© Leaders in Security – LSEC – 3IF.be, 2017, Public – Closed User Group Distribution, p 35

Source: AIOTI, 2017

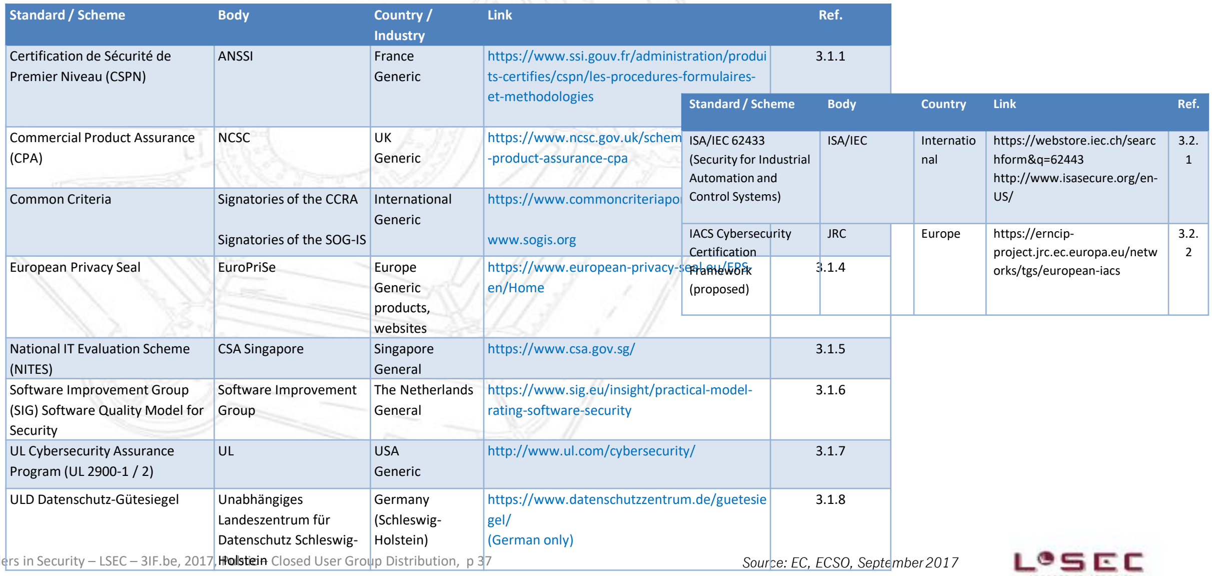
Even more standards : open source



© Leaders in Security – LSEC – 3IF.be, 2017, Public – Closed User Group Distribution, p 36

Source: AIOTI, 2017

Just Security Standards … over 100 of them



Standard / Scheme	Body	Country / Industry	Link	Ref.
Certification de Sécurité de Premier Niveau (CSPN)	ANSSI	France Generic	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies	3.1.1
Commercial Product Assurance (CPA)	NCSC	UK Generic	https://www.ncsc.gov.uk/schem-product-assurance-cpa	
Common Criteria	Signatories of the CCRA Signatories of the SOG-IS	International Generic	https://www.commoncriteriapo www.sogis.org	
European Privacy Seal	EuroPriSe	Europe Generic products, websites	https://www.european-privacy-seal.eu/EPS-en/Home	3.1.4
National IT Evaluation Scheme (NITES)	CSA Singapore	Singapore General	https://www.csa.gov.sg/	3.1.5
Software Improvement Group (SIG) Software Quality Model for Security	Software Improvement Group	The Netherlands General	https://www.sig.eu/insight/practical-model-rating-software-security	3.1.6
UL Cybersecurity Assurance Program (UL 2900-1 / 2)	UL	USA Generic	http://www.ul.com/cybersecurity/	3.1.7
ULD Datenschutz-Gütesiegel	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany (Schleswig-Holstein)	https://www.datenschutzzentrum.de/guetesiegel/ (German only)	3.1.8

Standard / Scheme	Body	Country	Link	Ref.
ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/	3.2.1
IACS Cybersecurity Certification Framework (proposed)	JRC	Europe	https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs	3.2.2

Source: EC, ECSO, September 2017

Certification than – Cybersecurity Act (COM(2017) 477) 09.17

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification

- Cybersecurity certification of ICT products and services
- ICT products and services need to directly incorporate security features in the early stages of their technical design
- purpose to inform and reassure purchasers and users about the security properties
- Proposal for Cybersecurity Certification Framework (the "Framework")

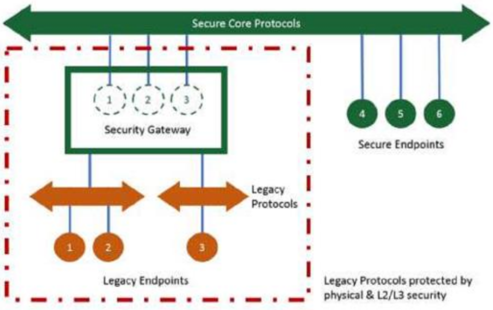
Source: EC, September 2017

IIC ISF Standard : Applying Security on the 3-tier architecture

Secure Implementations

End-to-end security: To achieve end-to-end security in an IIS, its implementation must provide:

- protected **device-to-device** communications,
- **confidentiality and privacy** of the data collected,
- **remote** security management and monitoring,
- simultaneously addressing **both existing technologies** as well as **new technologies**, and
- seamlessly spanning both information technology **(IT)** and operational technology **(OT)**
- **subsystems and processes** without interfering with operational business processes.



Source: IIC, 2016

Recommended : Industrial Internet (IIC) Security Framework Architecture

The Industrial Internet effort will bring industrial control systems online to form large end-to-end systems, connecting them with people, and fully integrating them with enterprise systems , business processes and analytics solutions. These end-to-end systems are referred to as Industrial Internet Systems (IISs).

Industrial Internet Reference Architecture

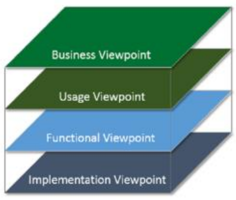


Figure 3-2 Architecture Viewpoints

Security across Viewpoints

1. Integrated approach
2. Threat modelling and secure design

Security concerns in Business context

Usage Viewpoints

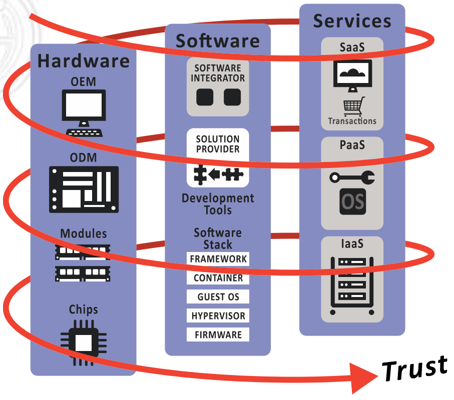
Common Security Common Security Activities

1. Security monitoring
2. Security auditing
3. Security policy management
4. Cryptographic support management

Functional Viewpoint

Common Security Functions

1. Security audit
2. Identity verification
3. Cryptographic support
4. Data protection and privacy
5. Authentication and identity management
6. Physical protection

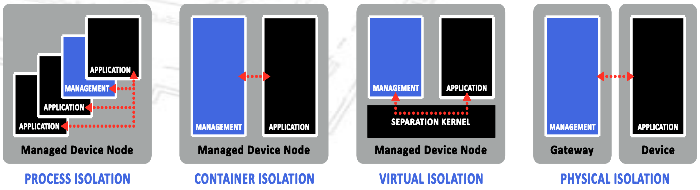


Source: IIC, 2016

IIC IIoT Security Reference Architecture Components

- Security Isolation Models
- Process Isolation
- Container Isolation
- Virtual Isolation
- Physical Isolation

- Future :
  - Decentralized Management
  - Edge Autonomy
  - Software Defined World
  - Hardware Identity (PUF)
  - Privacy Controls: Homomorphic Encryption
  - Quantum Computing
  - Fog Computing, Blockchain



© Leaders in Security , LSEC - 3IF, 2017, Public – Closed User Group Distribution, p 41

Source: IIC, 2016

LSEC – European Cyber Security Catalyst

European Network of Security Professionals, Research and Industry

LSEC is an international IT - & Information **Security cluster**, a **not for profit** organization that promotes Information Security and the expertise in Europe. Founded by **KU Leuven**, supported by **European** and **Flemish** Communities and leading a PAN European Private partnership that interacts with Public Institutions, LSEC connects security experts, research institutes and universities, government agencies, end users, funding bodies and technical experts and is a **catalyst in cyber security innovations**. LSEC activities aim to raise cyber security **awareness**, support innovation and improve the competitiveness of the IT- Security market.

Unite stakeholders, stimulate collaboration, enable high tech entrepreneurship

LSEC provides an international platform that unites security stakeholders, stimulates collaboration and enables high tech entrepreneurship. This will help researchers understand industry needs, help Industry access the IT security research that they need, and help ensure that fundamental research is translated to sustainable solutions.

© Leaders in Security – LSEC, 2017, Private & Confidential – Closed User Group Distribution – Do Not Distribute

LSEC – European Cyber Security Catalyst

Bring together the IT Security Expertise in Europe

With a broad membership base of over 265+ security specialized organizations, and more than 8.000 individual Information security professionals, LSEC accesses over 25.000 security stakeholders on a regular basis. With operations in the Netherlands, Belgium, Luxembourg and the UK, LSEC leads a PAN European Partnership with other security clusters that interacts with private partners, policy makers and public administration.

Strategic partner to FHI

LSEC has a strategic partnership with other European Cyber Security Clusters and Industry Associations. We've teamed up with FHI & D&E, because of joint interests and experience sharing, providing a channel for collaboration and joint developments.

eTrade Summit 2017

TRENDS IN CYBERSECURITY

(relevant for SafeShops.be)

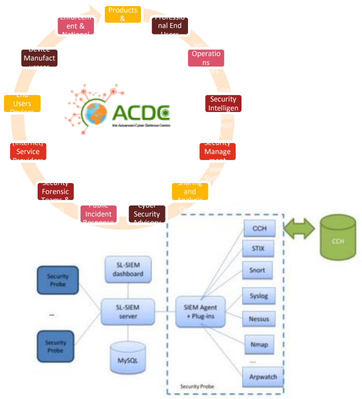
LSEC Activities :

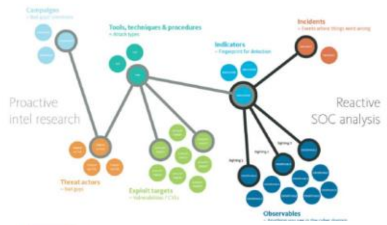
1. By Members for Members :
Experience Sharing - Conferences, Seminars, Workshops, Education, Training

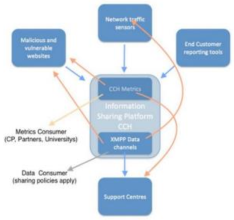
LSEC Data Protection
General Data Protection Regulation
Use Cases for DPIA & PbD Workshops
CYBER RANGE

LSEC Activities :

2. Cyber Security Threat Intelligence Sharing Platforn





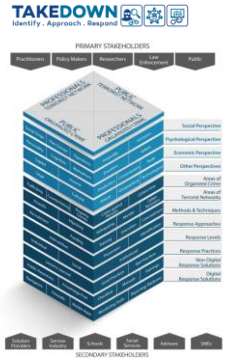

Network traffic sensors
Malicious and vulnerable websites
End Customer reporting tools
CCH Metrics
Information Sharing Platform CCH
XMPP Data channels
Metrics Consumer (CP, Partners, Universitys)
Data Consumer (sharing policies apply)
Support Centres

LSEC Activities :

3. Industrial Collaborations

IPACSO Innovation Awards

IPACSO AWARDS
Jakub Boratynski
Head of the Trust Unit, DG CONNECT, of the European Commission
EUROPEAN CLOCK
IPACSO



Industrie 4.0, Industrial Internet and Industrial IoT in Flanders

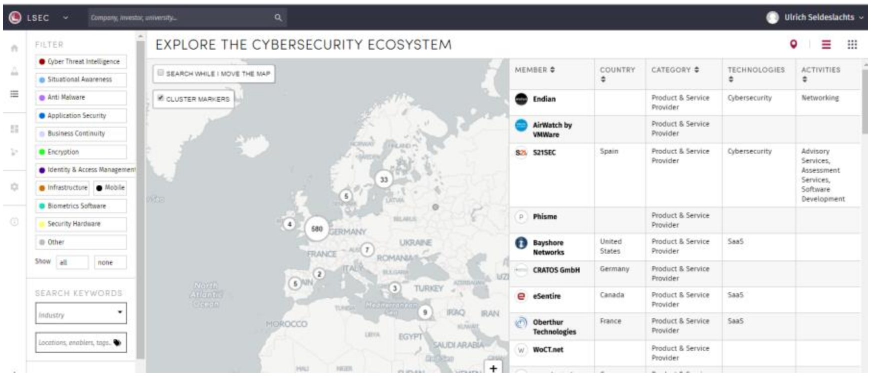
Are You..?

Manufacturer, Industrial Processor or Technology Provider
Small & Medium Sized
Going Smart, Digital and Connected

White Paper

Security in
Industrie 4.0
Industrial Internet
Industrial IoT

LSEC European Market Platform : Clusters going digital



EXPLORE THE CYBERSECURITY ECOSYSTEM

FILTER

- ● Cyber Threat Intelligence
- ● Situational Awareness
- ● Anti Malware
- ● Application Security
- ● Business Continuity
- ● Encryption
- ● Identity & Access Management
- ● Infrastructure
- ● Mobile
- ● Biometrics Software
- ● Security Hardware
- ● Other

Show all none

SEARCH KEYWORDS

Industry

Locations, enablers, tags...

□ SEARCH WHILE I MOVE THE MAP

☑ CLUSTER MARKERS

MEMBER ⬍	COUNTRY ⬍	CATEGORY ⬍	TECHNOLOGIES ⬍	ACTIVITIES ⬍
Endian		Product & Service Provider	Cybersecurity	Networking
AirWatch by VMWare		Product & Service Provider		
S21SEC	Spain	Product & Service Provider	Cybersecurity	Advisory Services, Assessment Services, Software Development
Phisme		Product & Service Provider		
Bayshore Networks	United States	Product & Service Provider	SaaS	
CRATOS GmbH	Germany	Product & Service Provider		
eSentire	Canada	Product & Service Provider	SaaS	
Oberthur Technologies	France	Product & Service Provider	SaaS	
WoCT.net		Product & Service Provider		

GLOBAL EPIC
Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity

PARTNERSHIP MEMBERS

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

cyberspark ISRAELI CYBER INNOVATION ARENA

Carleton UNIVERSITY Canada's Capital University

GCR

UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK Canadian Institute for Cybersecurity

HSD The Hague Security Delta

THE KOSCIUSZKO INSTITUTE

PROCOMER COSTA RICA exporta

Cyber Wales

Cámaras Fundación INCYDE

LSEC LEADERS IN SECURITY

POLITECNICO DI TORINO 1859 1906

CYBERTECH YOUR NETWORK EXPANDED

bwtech @UMBC RESEARCH & TECHNOLOGY PARK

CITY OF SURREY the future lives here.

https://globalepic.org

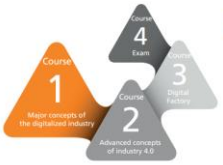
3IF.be – Industrie 4.0 in Flanders

1. **Stimulate** (economic) developments of industrial internet, industrie 4.0 and IIoT in Flanders, and support the viability of the Industry
2. **Inform** manufacturers and suppliers on use cases and technological developments to fully benefit of the technological opportunities ahead
3. **Support** the digital transformation with information sessions, workshops, trainings and advisory services
4. **Connect** suppliers with users of technology
5. **Identify and Create I4.0 ecosystems**, with Flemish technology providers
6. **Support** industry initiatives with digital, technology and best practice expertise and experiences
7. **Fieldlab Predictive Maintenance and Industrial Data System**

3IF.BE Trainings & Workshop : Drivers License I4.0 – also in Nederland

DIGITALISATION AND
INDUSTRY 4.0 DRIVER LICENSE®

Are you on target for industry 4.0?



Course 4
Exam
Course 3
Digital Factory
Course 1
Major concepts of the digitalized industry
Course 2
Advanced concepts of industry 4.0

Course 1 basics of the industrialisation, big data, IoT, horizontal and verticale integration, production 4.0, R&D 4.0, logistic 4.0, business-model-innovation 4.0

Course 2 maintenance procedures 4.0, quality management 4.0, staff and workplace 4.0, data mining, robotic 4.0, after sales services 4.0, autonomous systems

Course 3 assistance-systems, collaboration human-machine, cloud systems, system periphery / MES 4.0, additive production, engineering, options for implementation

Course 4 preparation and final examination for the industry 4.0 driver license

KEY QUESTIONS IN COURSE 1

- Why is it important to act early?
- How does digitalisation change the world?
- Which development paths are possible with industry 4.0?
- What new possiblities are created for the production environment, logistic and R&D?
- Why are new business models the actual challenge?

YOUR PROFIT

- systematic comprehension for the digitalisation
- concrete approaches for your company
- insights into already implemented industry 4.0 projects
- intensive interchange with other course participants and the trainer
- character of a interactive workshop

3IF.BE Digital Transformation Guidance

ACME

Industrieel Internet Transformatieplan

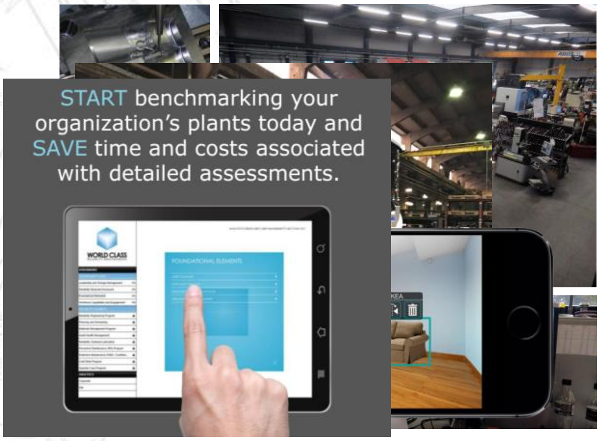
Richtlijnen, procedures, handleidingen en codes van goede praktijk voor Digitalisering van de Smart Factory, Industrie 4.0, Industrial Internet en Industrial IoT

Inzichten in de transformatie naar nieuwe ontwikkelingen en digitalisering van de productie

Door het 3IF.be (Industrial Internet in Flanders) en LSEC – Leaders in Security,
Voor productiebedrijven, integratoren en ICT-oplossingen-leveranciers

www.3if.be
www.lsec.eu

© Analyn bvba for LSEC – Leaders in Security, June 2016 p. 1/65



START benchmarking your organization's plants today and SAVE time and costs associated with detailed assessments.

Assessments for Manufacturing SME's in 2017-2018

Save the Date

www.lsec.eu – www.3if.be

3IF.be

29-30.05.18

Industrie 4.0 – Industrial Internet in Flanders
International Conference 2018

- Trends & Developments in Industrie 4.0 & IIoT
- From Use Case to Business Case to Industrial Roll Out and Operations
- Edges and Cloud, Mastering End to End Security
- Flanders Industrie 4.0 Field Lab experiences from the trenches.

Conclusions for Electronics & Design Manufacturers :

1. Enterprise & Industrial IoT are being accepted, already omnipresent and growing
2. Simple and basic security measures are not always included : security by default
3. IIoT impacts current business and causes security challenges for others
4. Different standards and certification mechanisms, not always aligned
5. Reference Architectures exist and are being further enhanced
6. Regulation under development
7. Allow to Integrate in existing Security Frameworks such as IAM and GRC where possible
8. Security by default, Security by design
9. End to End
10. Isolation & Segmentation

Cybersecurity and Operational Design & Efficiency
should be considered - evaluated together

Industrie 4.0, Industrial Internet and Industrial IoT in Flanders

Are You..?

Manufacturer, Industrial Processor or Technology Provider
Small & Medium Sized
Going Smart, Digital and Connected

Q or C
Ulrich Seldeslachts
ulrich@lsec.eu
+32 475 71 3602