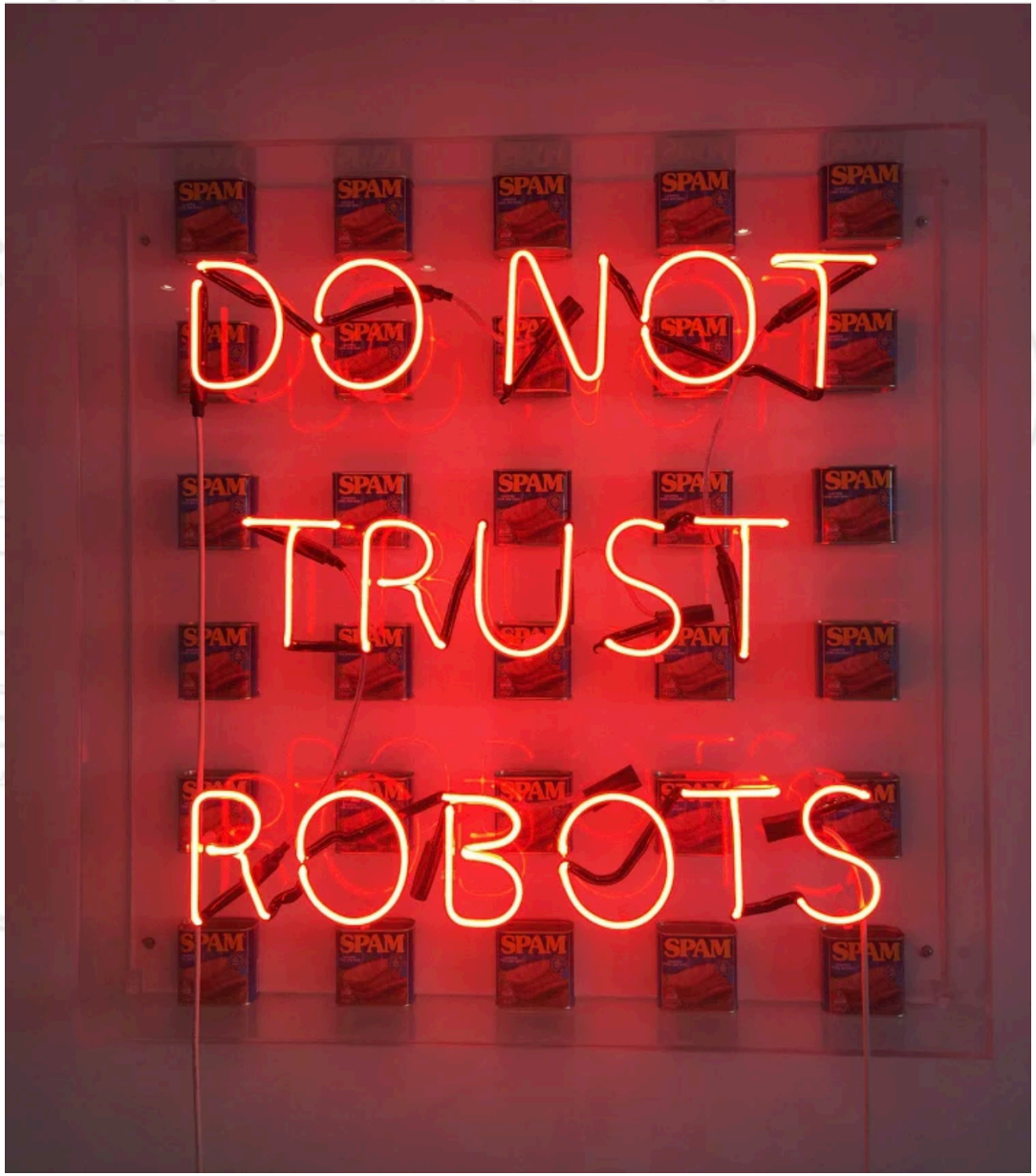

HACKED
shutterstock.com • 313538906

CSfR
CYBERSECURITY FOR ROBOTICS
www.cybersecurityforrobotics.com

www.cybersecurityforrobotics.com

Home About CyberSecurity Research Robots Conference2019 Recommendations Partners Experts News



Source : Half A Roast Chicken, Eve De Haan, 2018

TRINITY DIH

A Network of Digital Innovation Hubs in Advanced Robotics

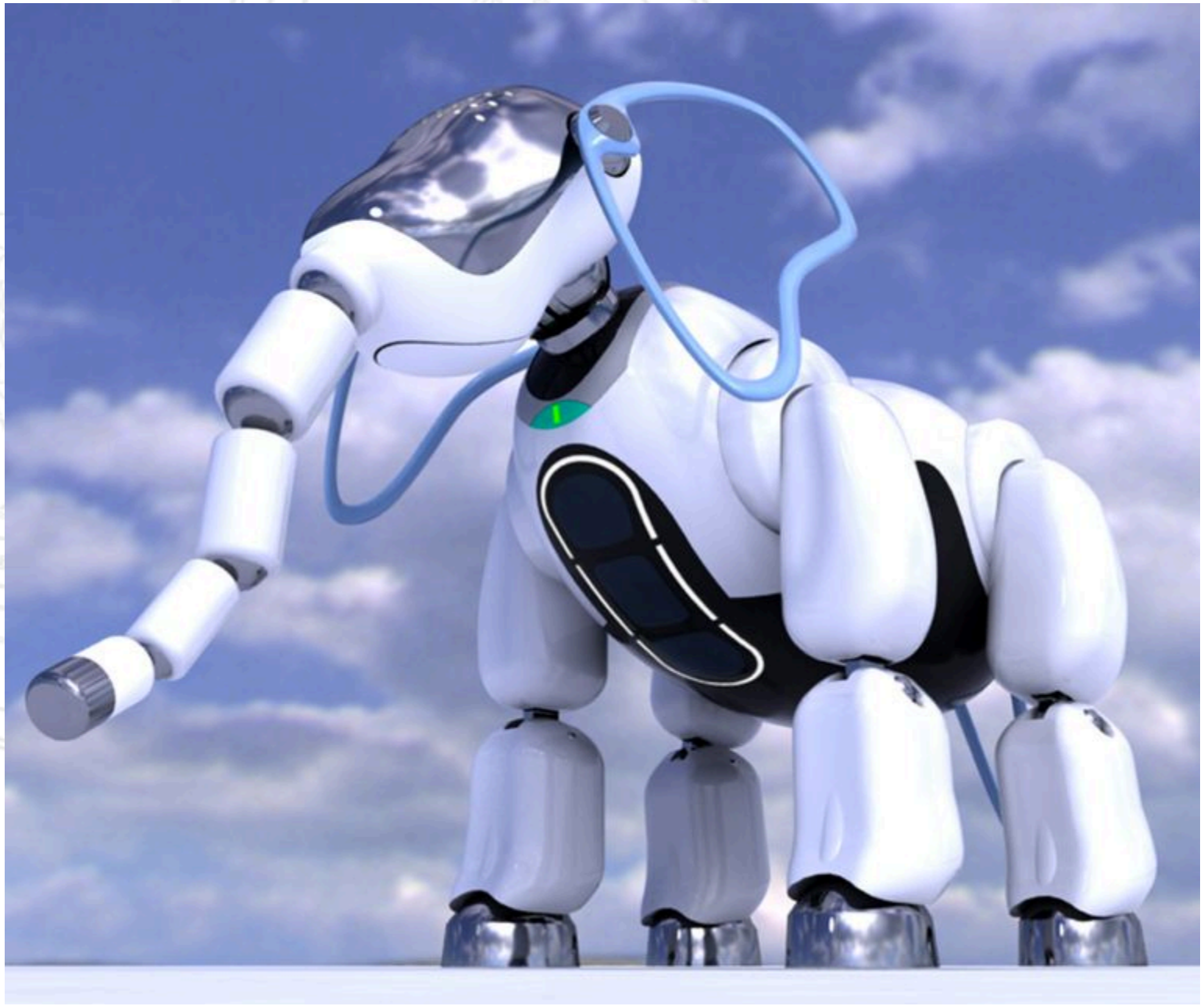
FUNDS UP TO
€300K
per team

TAKES
0%
equity

A network of Digital Innovation Hubs supporting manufacturing SMEs to become more competitive through robotics and digital technologies!

Why TRINITY?

There is a huge opportunity for manufacturers to adopt new robotics and IoT technologies



Agenda CyberSecurity for Robotics at ERF 2020

14.00 Relevance of CyberSecurity for Robotics : putting the Elephant in the Room

Introduction :	Endika Gil Uriarte, Alias Robotics
Current security threat landscape in robotics,	Víctor Mayoral, Alias Robotics
Detection anomalies in CPS environments: Results from the IoT4CPS project.	Arndt Bonitz, AIT
Robotics honeypots: Learning from robot hackers.	Francisco Lera, University of León
Attacking mobile robot bases	Bernhard Dieber, Joanneum Research





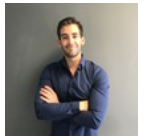

15.00 Discussion - Debate & Interactive Workshop

with Francesco Ferro, Pall Robotics

Agenda CyberSecurity for Robotics at ERF 2020

16.15 CyberSecurity for Robotics Solutions : cutting the Elephant into Pieces

Security in ROS & ROS 2 robot setups — Víctor Mayoral Vilches, Alias Robotics



Access Control Models, with Applications to Robotics, — Stefan Rass, Uni of Klagenfurt (AAU)

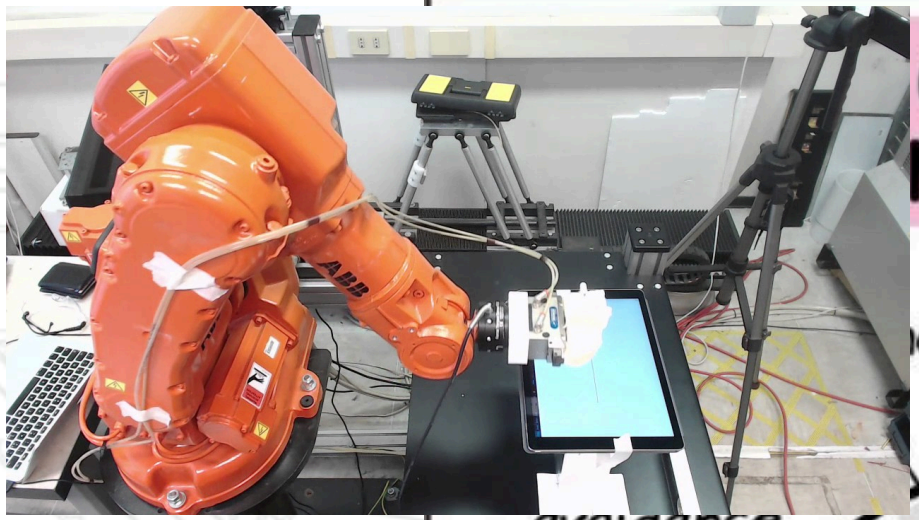
SecDevOps & Agile Development, Embedded and other Security Solutions, — Ulrich Seldeslachts, LSEC – Shift Left, SKUDO

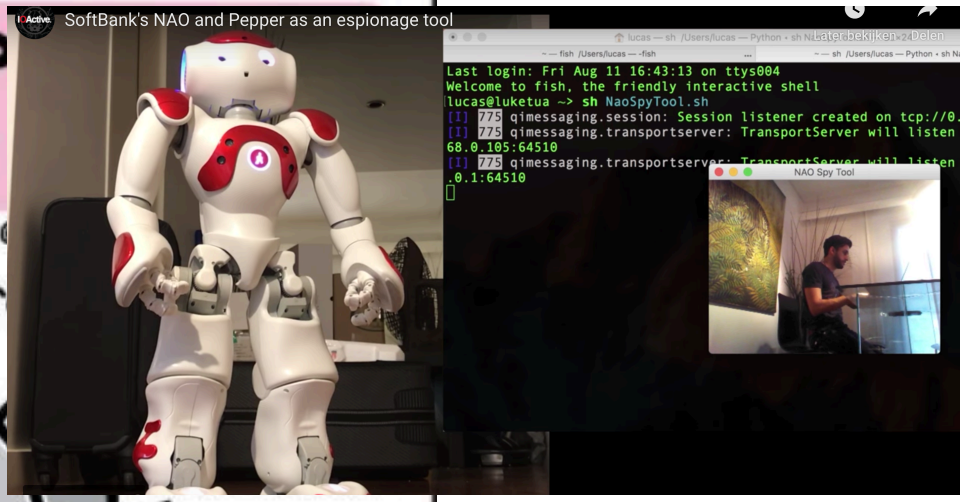
17.15 Discussion - Debate & Interactive Workshop

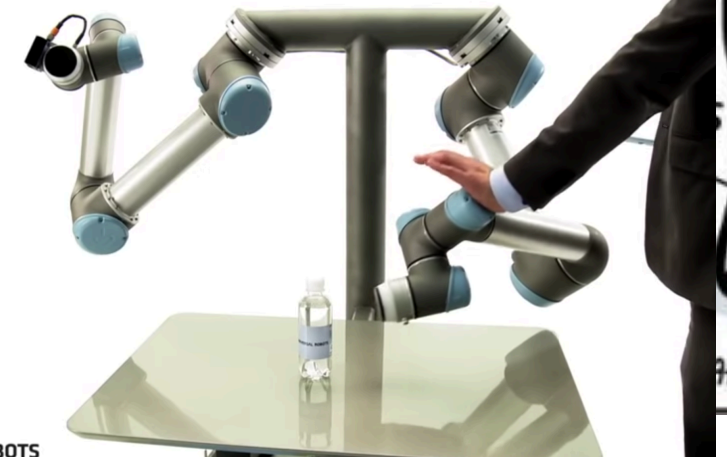
Robot Security Survey, Endika Gil Uriarte, Alias Robotics

CyberSecure Robot Development – Slicing the Elephant

NOT ONLY MANUFACTURER's RESPONSIBILITY







Recent Events : nothing sophisticated

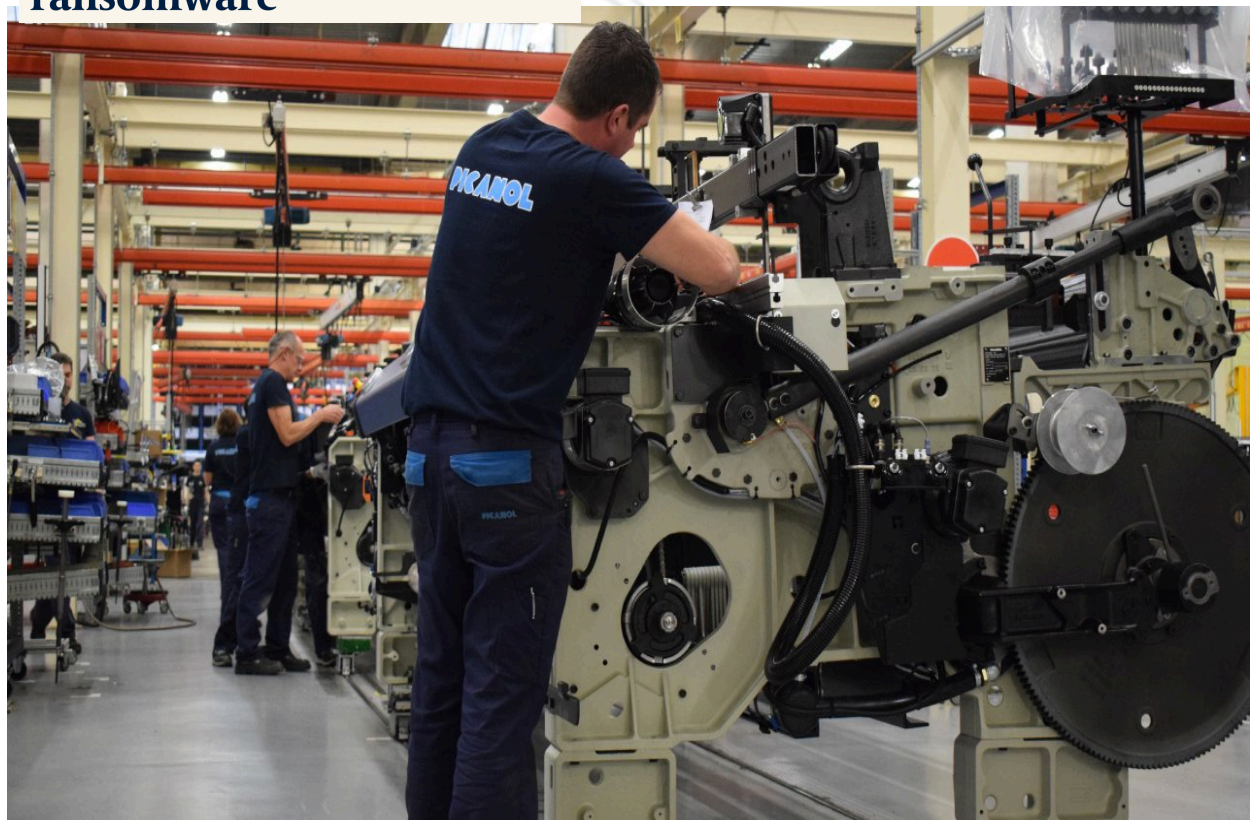
Asco closure after cyber-attack to last another week

Saturday, 22 June 2019

© Belga

Asco, the Zaventem-based company that makes aircraft parts, will now remain closed at least until 28 June, following a cyber-attack two weeks ago.

Picanol mogelijk grootste Belgisch slachtoffer ransomware



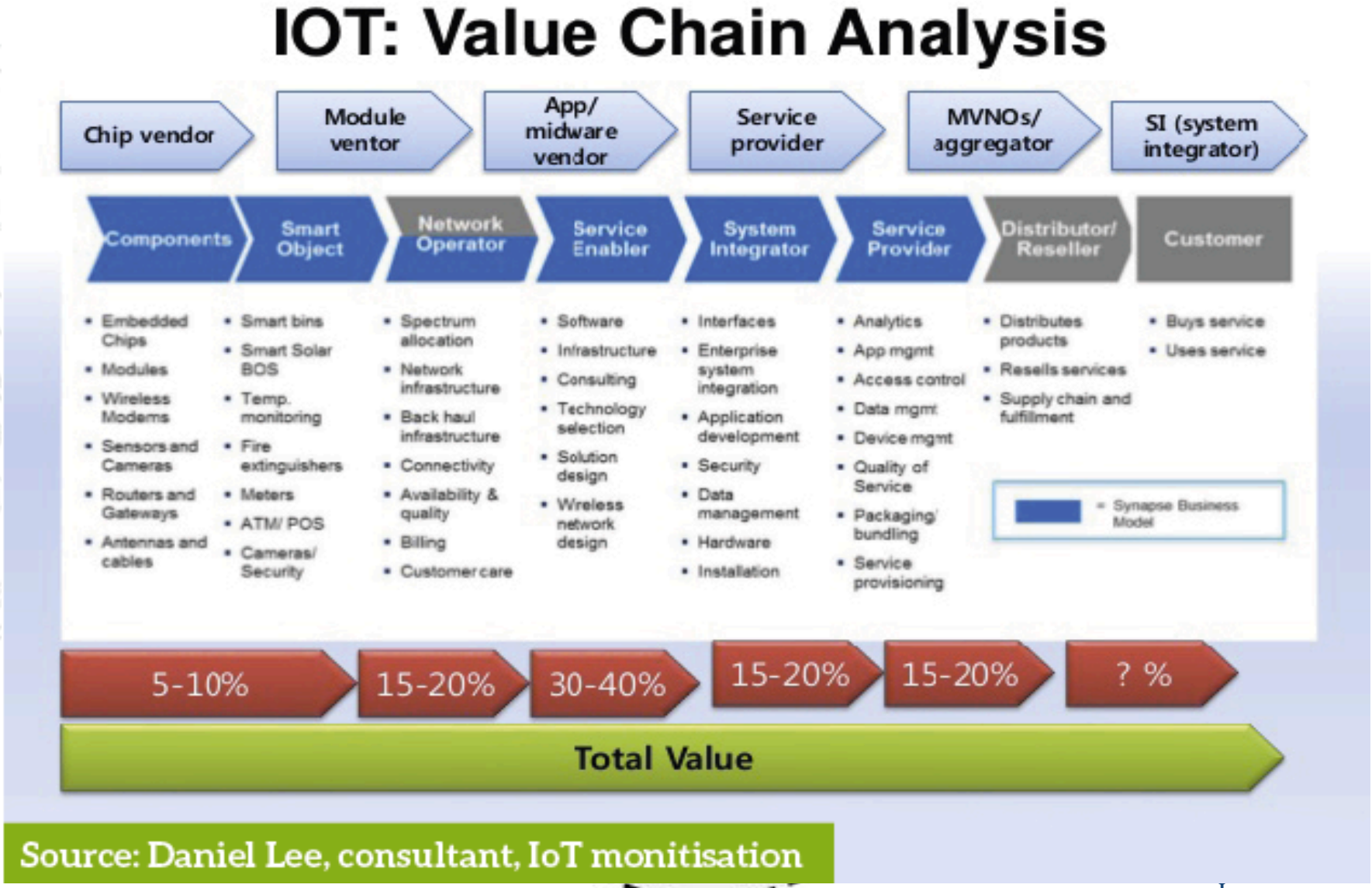
WIM DE PRETER, MARIE VAN OOST | 14 januari 2020 00:16

Source : Stormshield, The Register, Brussels Times, , Tijd

BUT END USER / MANUFACTURER / OPERATOR WILL BE MAINLY IMPACTED

CyberSecure Robot Development – Slicing the Elephant

Whole Robotics Value Chain & Ecosystem responsible & affected by CS



Sources : DxC, Daniel Lee, Harvard Business,

CyberSecure Robot Development – Masterplan Objectives WP

1. Safety of the user(s)
2. Consider users not trusting robots – AI & automation, ethics & privacy
3. Align to existing CyberSecurity frameworks and guidance
4. Bringing ecosystem and all stakeholders together : policy makers, manufacturers, users, integrators, industry, developers, operators

5. Liaise, reaching out to partners, partner constituencies
6. Formalizing Collaborations
7. Develop and Maintain Industry Guidelines, SBOM / Design / RIM ..
8. Educate and Awareness
9. Innovate and Research
10. Advocate & Promote CyberSecured Robotics

* Thanks to Oasis …

To obtain CyberSecure Robots

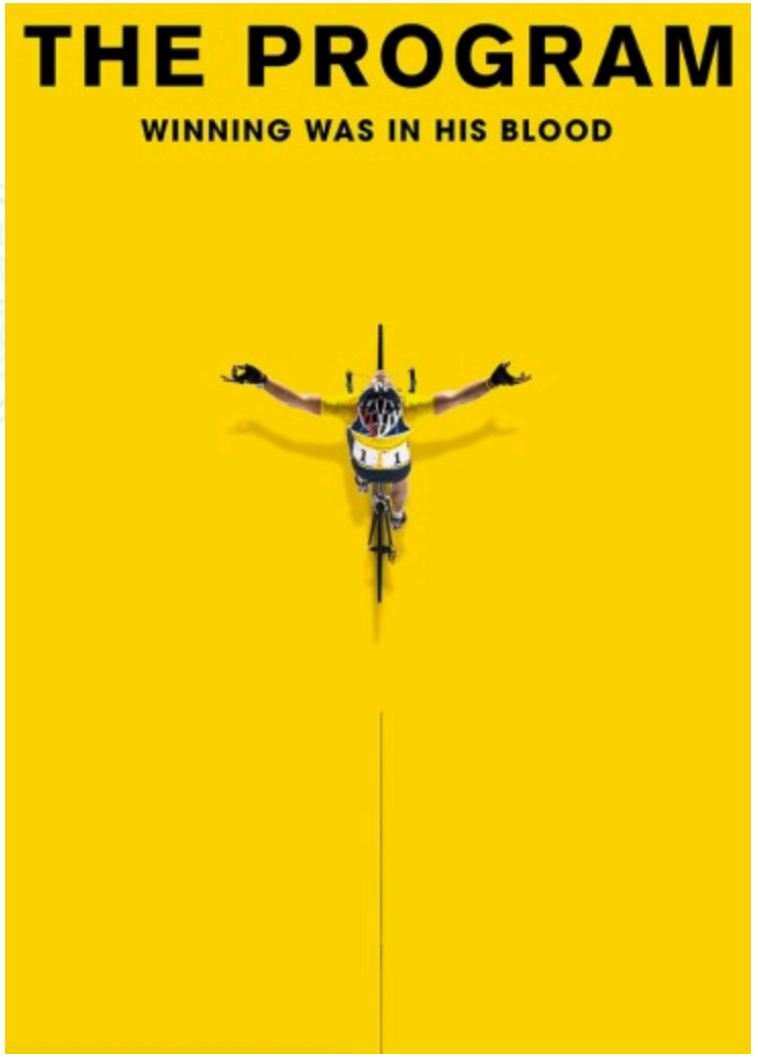
We need to …

Developers, Manufacturers, Integrators, End Users – Operators, …

* Thanks to Oasis …

CyberSecure Robot Development Program – CS by Design Program

1. Pre-market Guidance
2. Shared Responsibility Model
3. Cybersecurity Product Management
4. Software Bill of Materials
5. Reference Integrity Manifest
6. Secure Components
7. CyberSecurity by Design – Reduce Regression testing time
8. Certification – Re-certification
9. Train Developers, Manufacturing Design, Threat Modelling, Train the Trainer
10. Postmarket severity of harm - CVSS – Common Vulnerability Scoring System
11. Responsible and Coordinated Disclosure
12. Active ISAC
13. CyberSecurity Safety Analysis Board
14. Incentivize
15. Patching



* Thanks to Studio Canal

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – premarket guidance

Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance

MANUFACT
TO CYBERSI

For Small and Medium-Sized Manufacturers

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Source : FDA 2020, NIST 2015, NIST 2018

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – premarket guidance

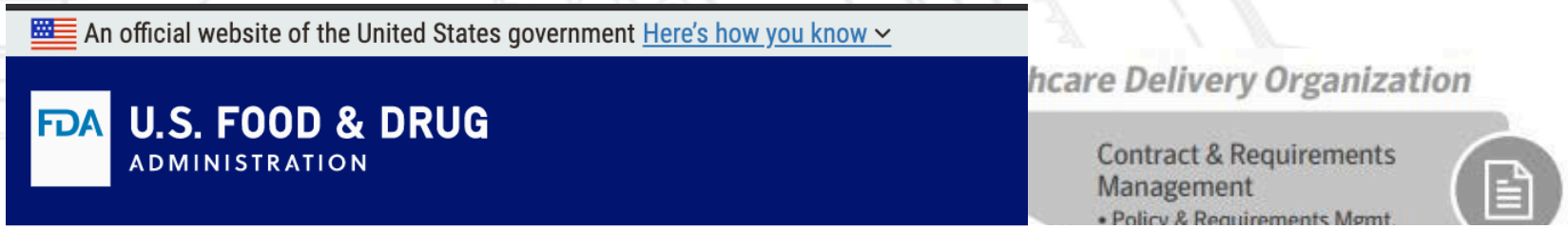
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

1. Identify and Protect Device Assets and Functionality
    1. Prevent unauthorized use : limit to trusted users and devices only
    2. Authenticate and check authorization of safety-critical commands
    3. Ensure trusted content by maintaining code, data, execution integrit
    4. Maintain Confidentiality of Data
2. Detect, Respond, Recover : Design Expectations
    1. Design the Device to detect cybersecurity events in a timely fashion
    2. Design the Device to Respond to and contain the impact of a potential cybersecurity incident
    3. Design the Device to Recover capabilities or services that were impaired due to a cybersecurity incident
3. Labeling Recommendations for Devices with Cybersecurity Risks
4. CyberSecurity Documentation
    1. Design Documentation
    2. Risk Management Documenation

Source : FDA 2020

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Shared Responsibility – healthcare devices example



← Home / Medical Devices / Digital Health / Cybersecurity

Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place.

- **Medical device manufacturers (MDMs)** are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.
- **Health care delivery organizations (HDOs)** should evaluate their network security and protect their hospital systems.
- **Both MDMs and HDOs** are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

Source : Symantec, 2016, FDA , 2020
https://www.researchgate.net/publication/325746918_CYBERSECURITY_FOR_HEALTHCARE_MEDICAL_DEVICES

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – CyberSecurity Product Management

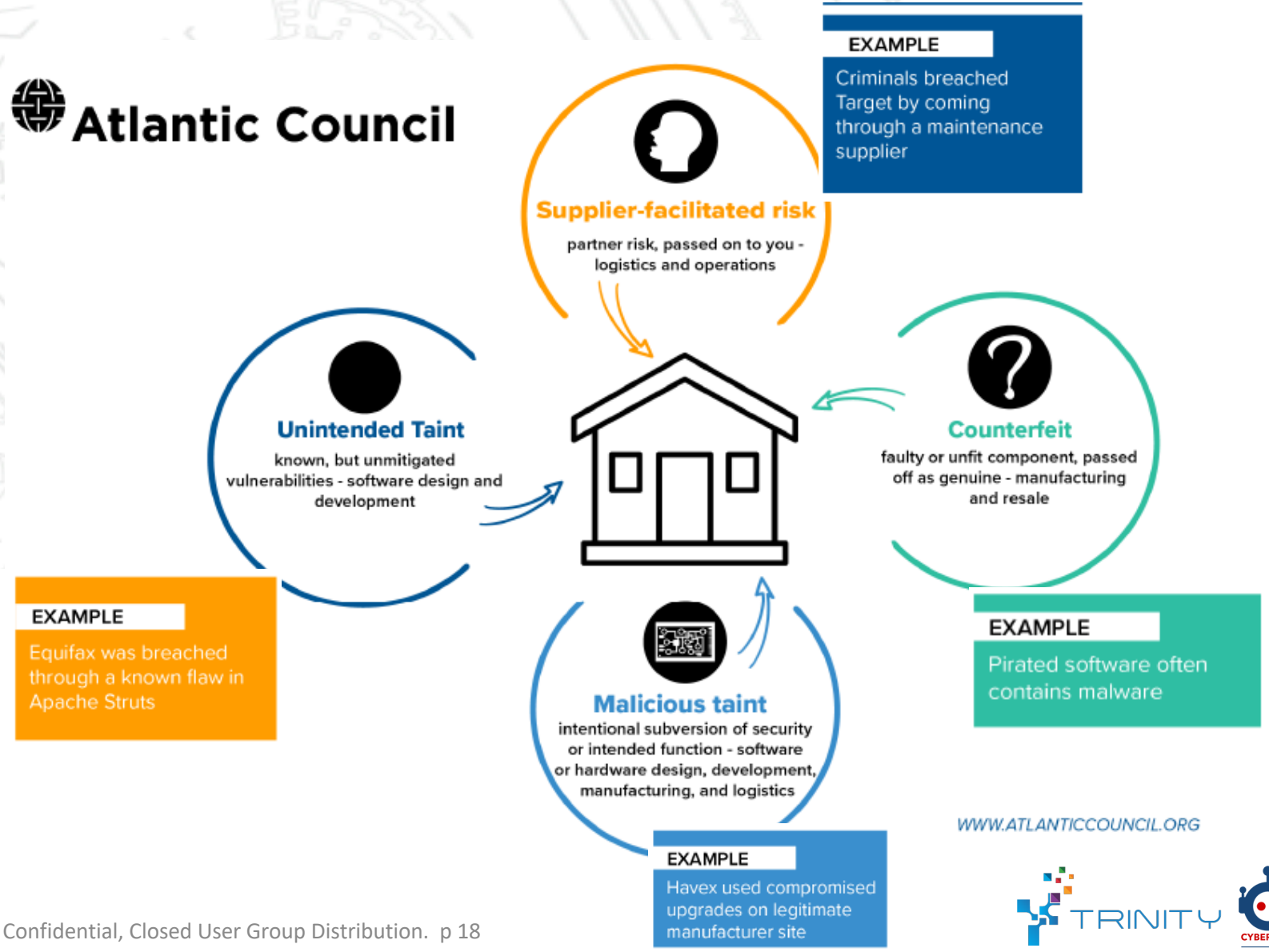
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

CyberSecurity Product Manager

- PM whose solution addresses information security needs of its customers.
- hands-on security practitioners, who've transitioned into product management
- built up their infosec prowess after becoming a PM by building upon their business, software engineering or other expertise
- empathize with risk-sensitive customers concerned about issues such as online threats, data safeguards, information security regulations, security incident handling, etc.
- answer questions related to your product's security domain, including: - measures are your prospective customers employing today to address the risks that your product tackles? How will your product's capabilities handle the ever-evolving threat and/or regulatory landscape? security benefits? operational burdens compare to the product's security value proposition? Security, compliance, audit or other roles benefit?

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Supply Chain Risk

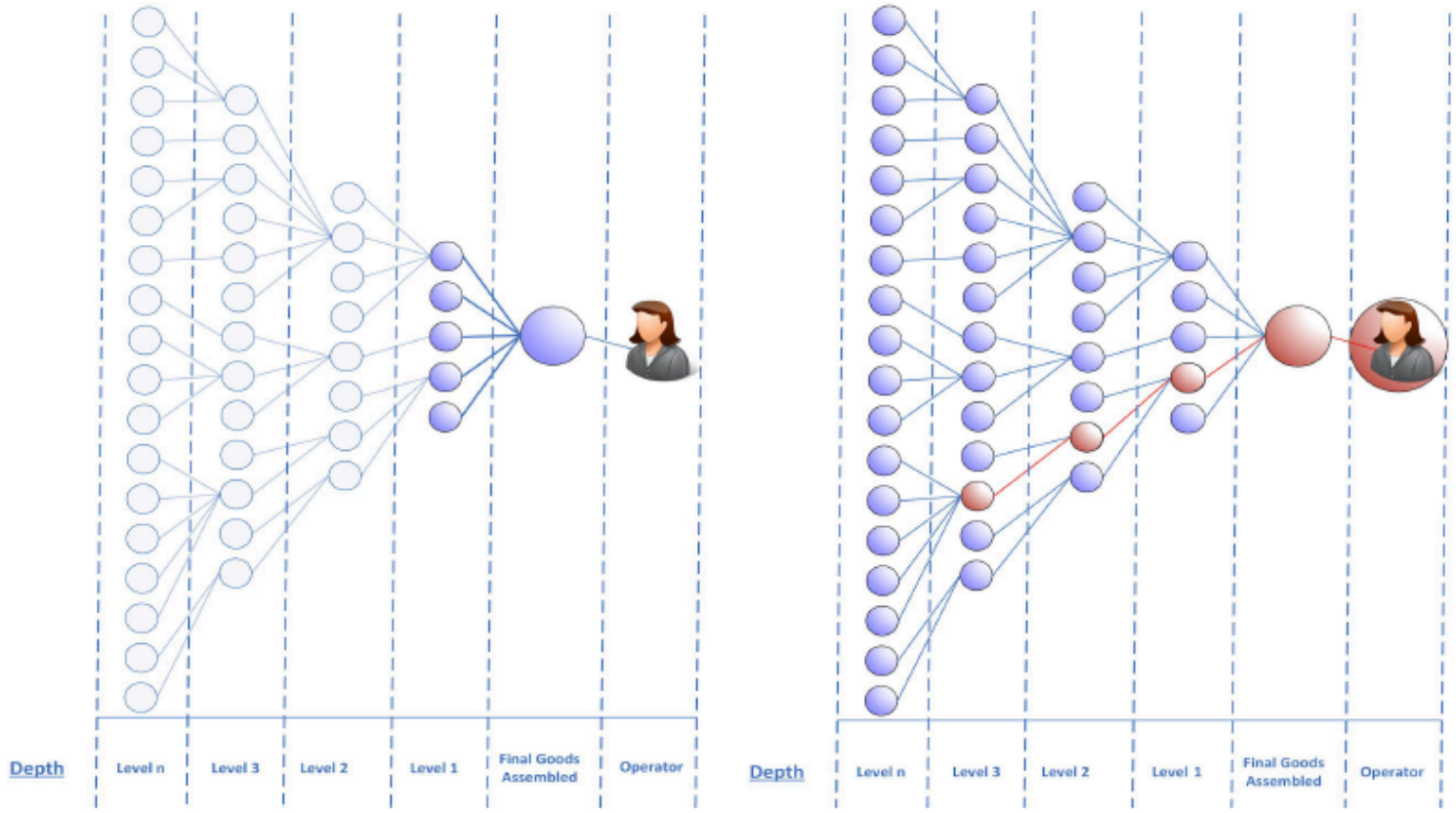


CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Software Bill of Materials

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Software Bill of Materials



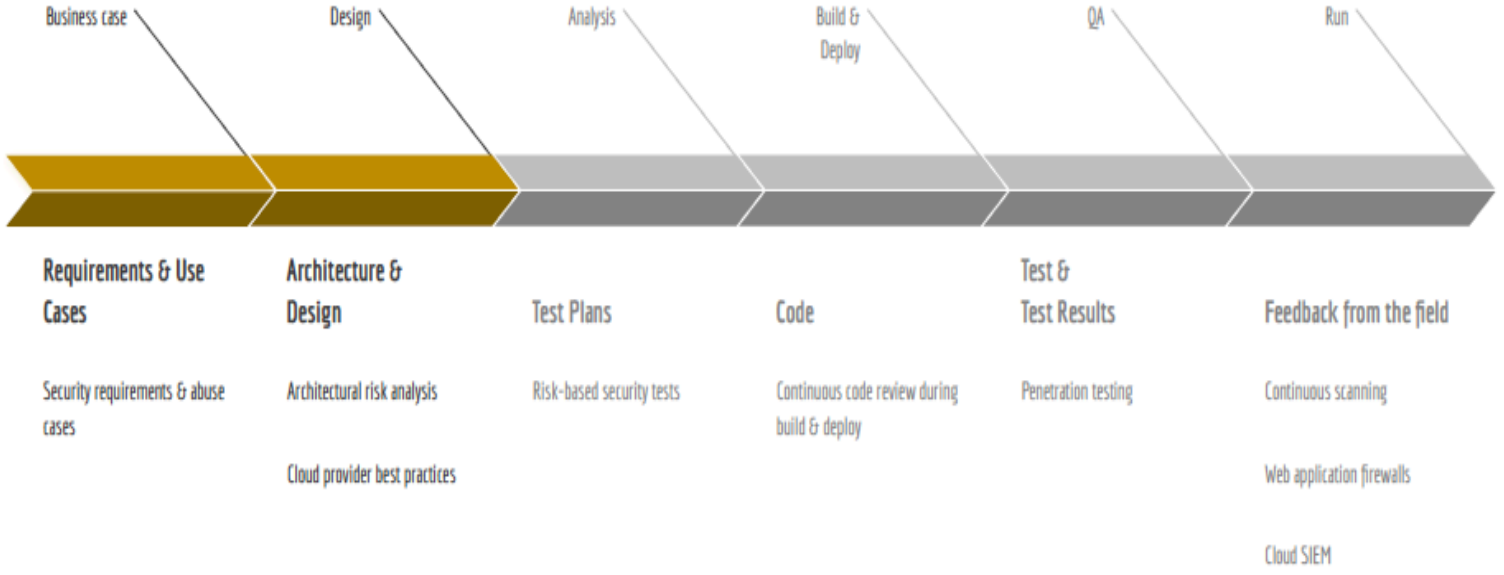
Limited visibility enables less awareness of risk

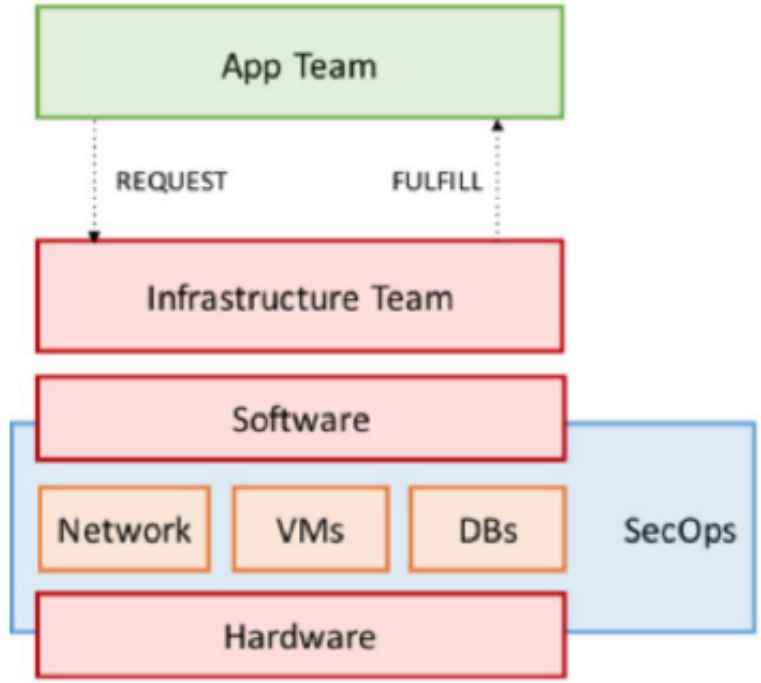
More complete visibility enables more complete awareness of risk

https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

CyberSecure Robot Development Program – CS by Design

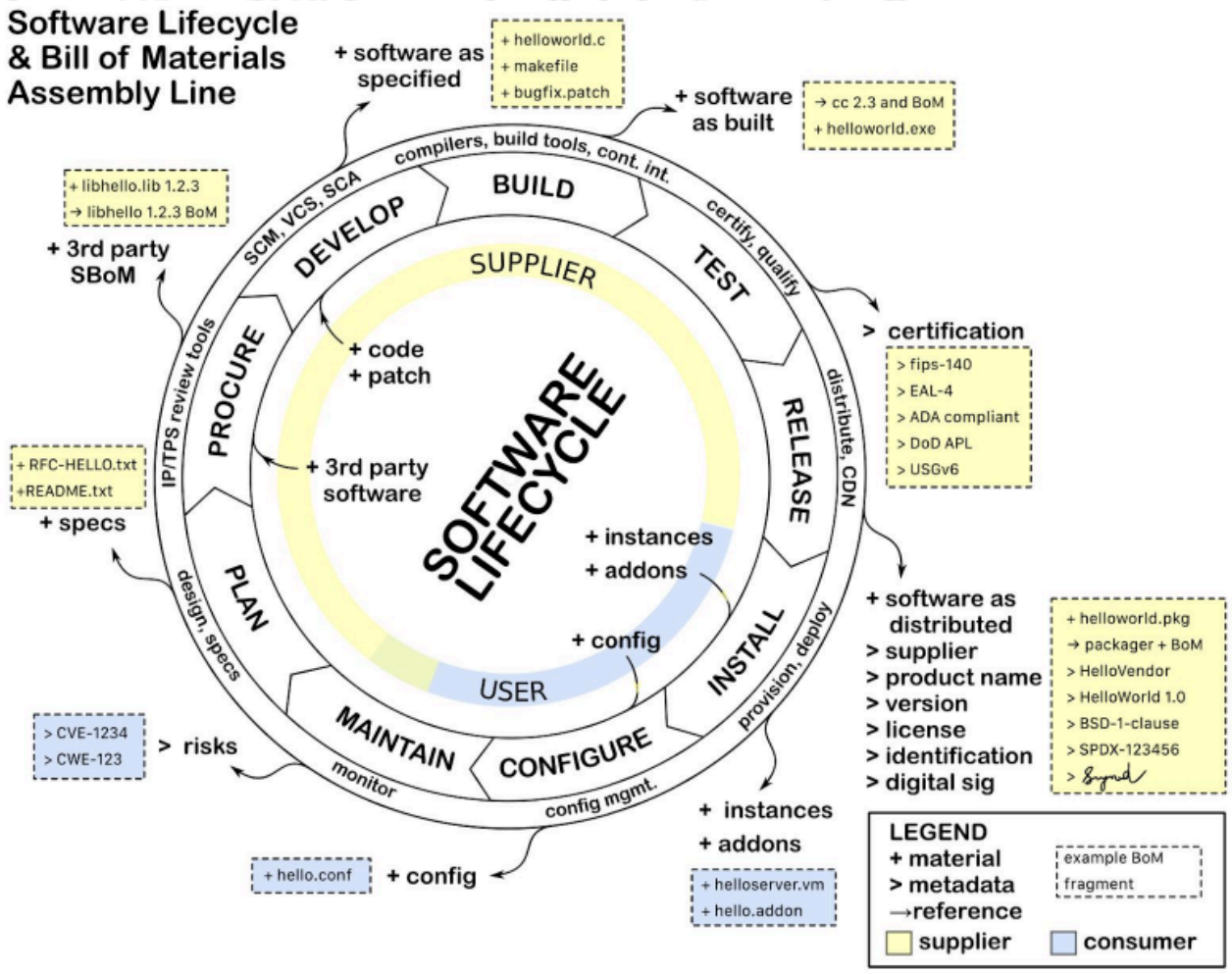
CyberSecurity by Design – Reduce Regression testing time





CyberSecure Robot Development Program – CS by Design

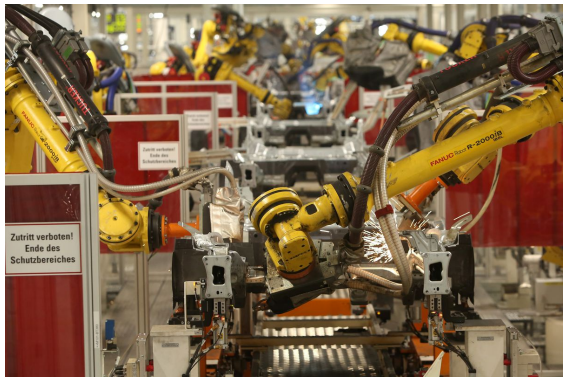
CyberSecurity by Design – Software Bill of Materials



https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

Industrial and Connected Robots : categorizing according to operation

Controller operated	the robot functionalities are being controlled by a robot controller, either integrated or separated from the robot arm or robot itself. Mostly the instructions to the robot are being sent in clear text.
PLC operated	the robot is being controlled through a PLC, typically connected to a central controlling environment, instructing directly the robots or sending instructions to the robot controller
ROS (1-2)	the (ROS) Robot Operating System v1 and 2 can directly instruct a number of robotic systems, and v2 is improving cybersecurity; but both systems have seen adoption in research projects, but only few in production and operational environments,
IoT	latest generation robots receive direct instructions from a series of microcontrollers integrated in the robot, running on an operating system utilizing internet technologies
Cloud Operated	new developments are taking place to have the robot receiving direct instructions from the cloud, requiring a continuous and constant internet connection to the robot. Instructions can be transformed from IoT to a robot controller or via PLC.



Source: LSEC, robots.com 2019

LSEC
LEADERS IN SECURITY

CyberSecure Robot Development Program – Responsible Disclosure

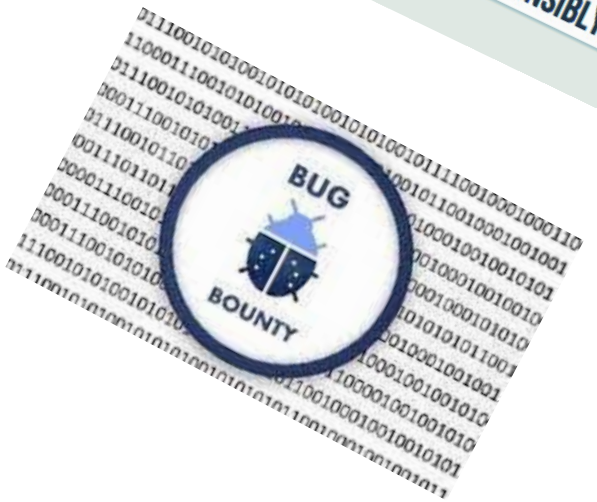
Buffalo NAS - 335 days in the wild without a patch

Disclosure timeline:

- 18-06-22: E-mail security contact listed on website.
- 18-07-02: E-mail security contact again.
- 18-07-03: Sent v
- 18-08-22: Sent C
- 18-11-06: Public
- **18-11-08: Public** **m.**
- 18-11-09: @Buff stream.
- ??-??-??: @Buff
- **19-09-16: ISE re** **per.**
- 19-09-18: Buffalo reaches out, provides reliable email.
- **19-10-09: Buffalo releases firmware v4.02.**

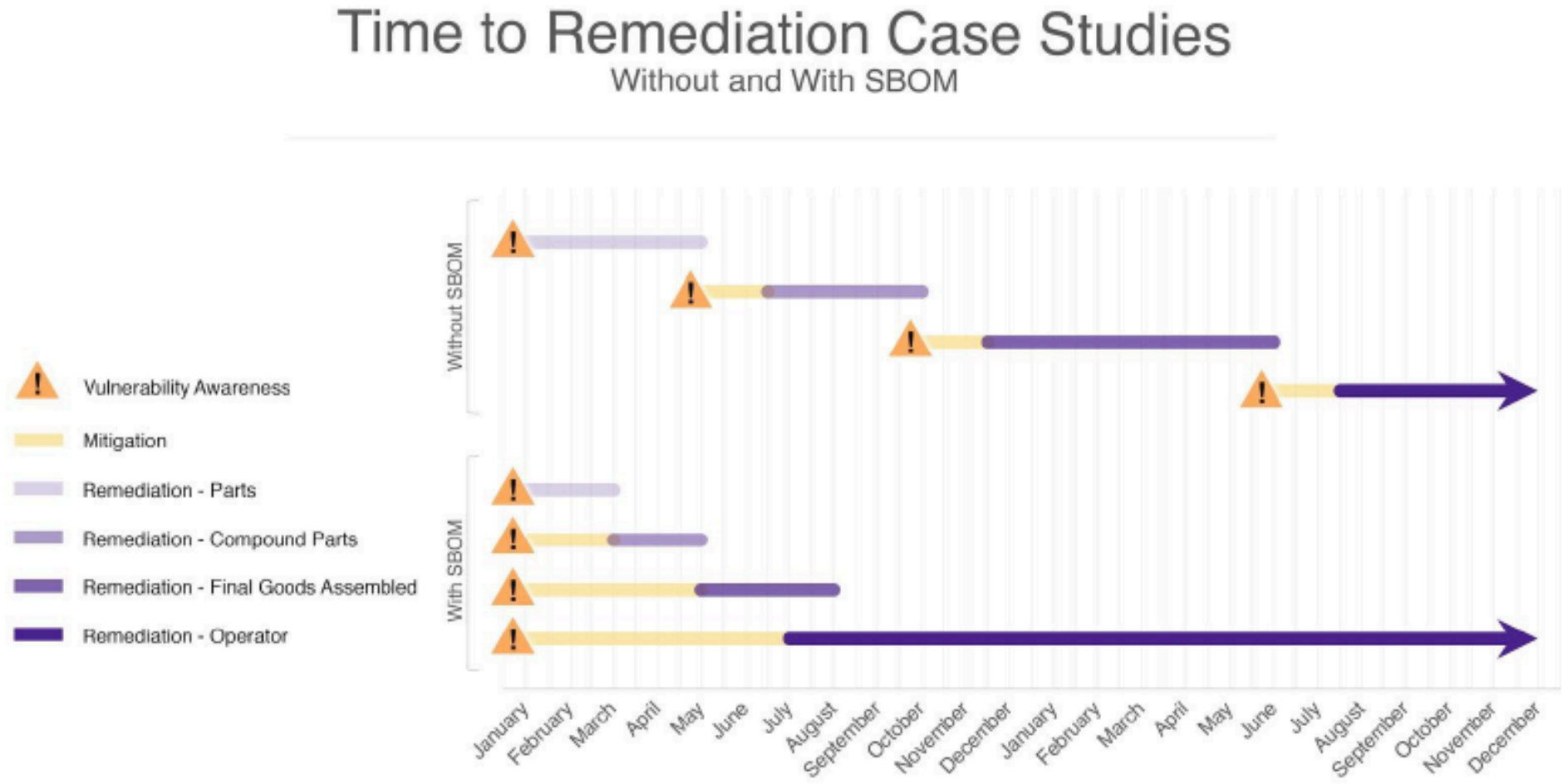
CS Robot Dev Program – Responsible Disclosure Manufacturers

1. Check your security inbox!
2. Social Media will hunt you down
3. If you don't have a public security point of contact, create one!
4. Bug bounty programs should not inhibit coordinated disclosure.
5. Audit your vulnerability disclosure resources.
6. Audit use of the X-Forwarded-For header.
7. Custom protocols are not an answer – researchers won't be intimidated by it
8. Remember that everyone makes mistakes.- Use them as opportunities to demonstrate integrity.



CyberSecure Robot Development Program – CS by Design

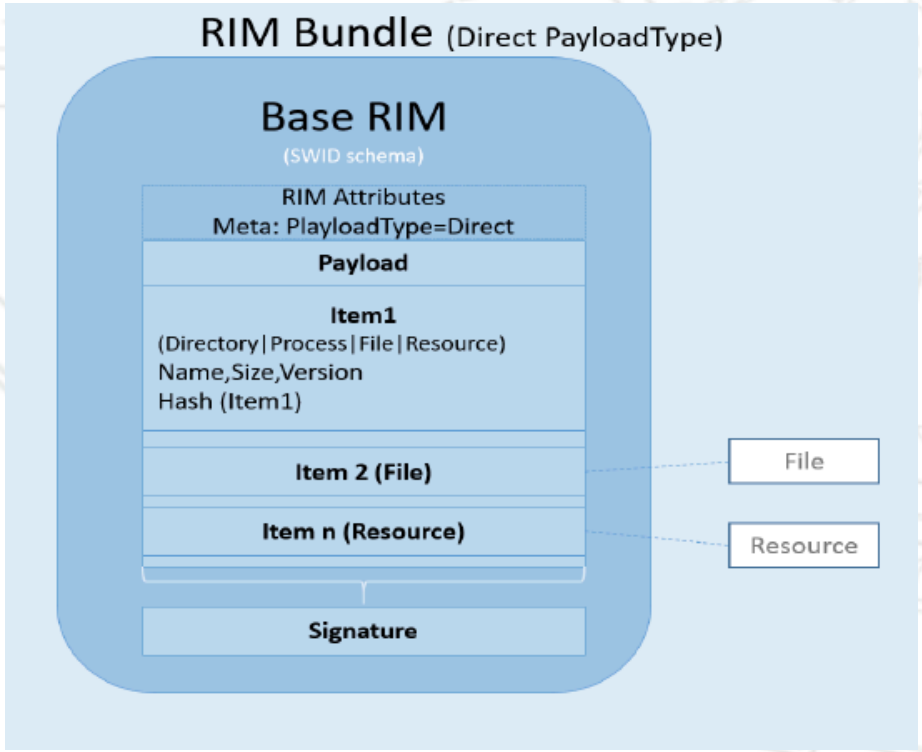
CyberSecurity by Design – Software Bill of Materials

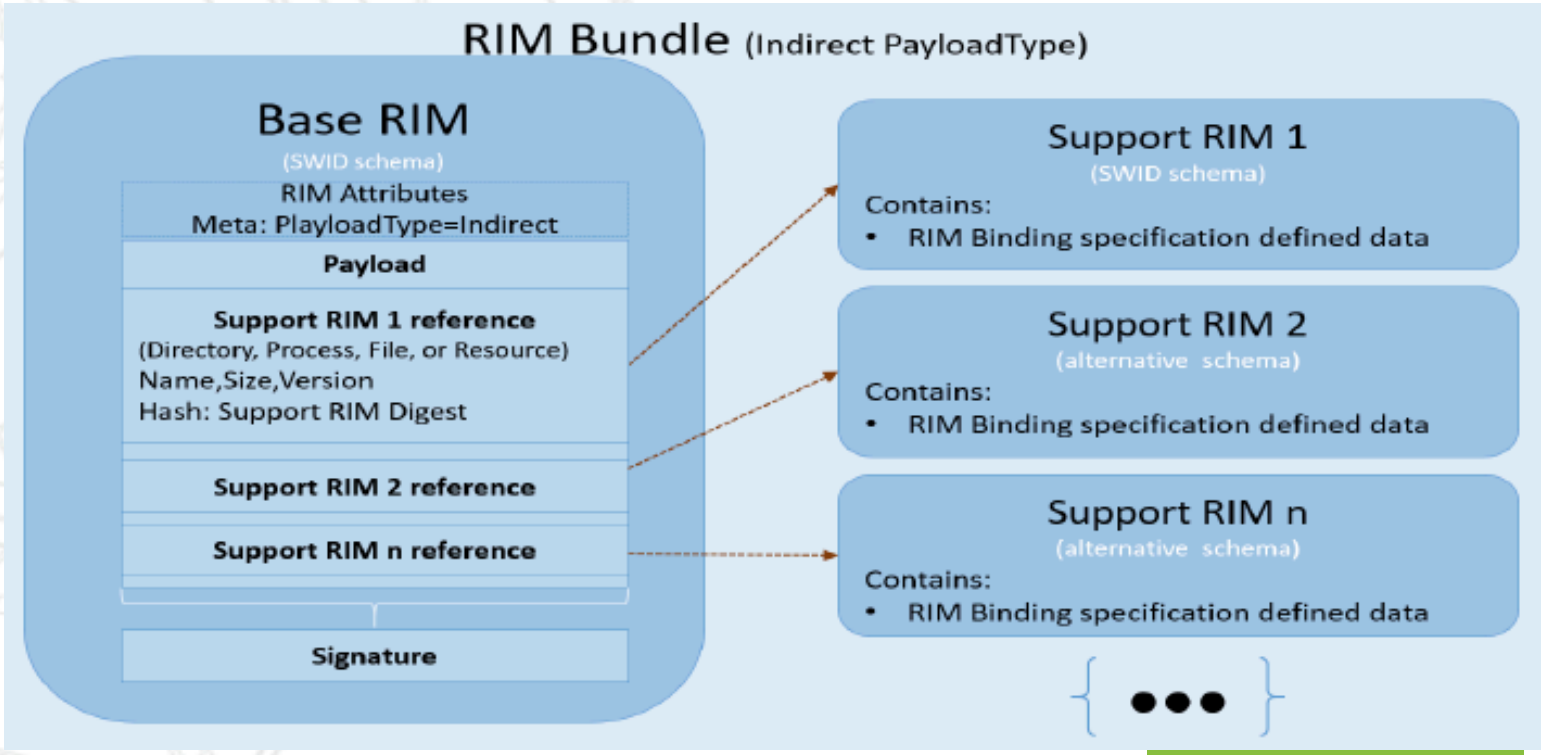


https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

CyberSecure Robot Development Program – RIM

Reference Integrity Manifest

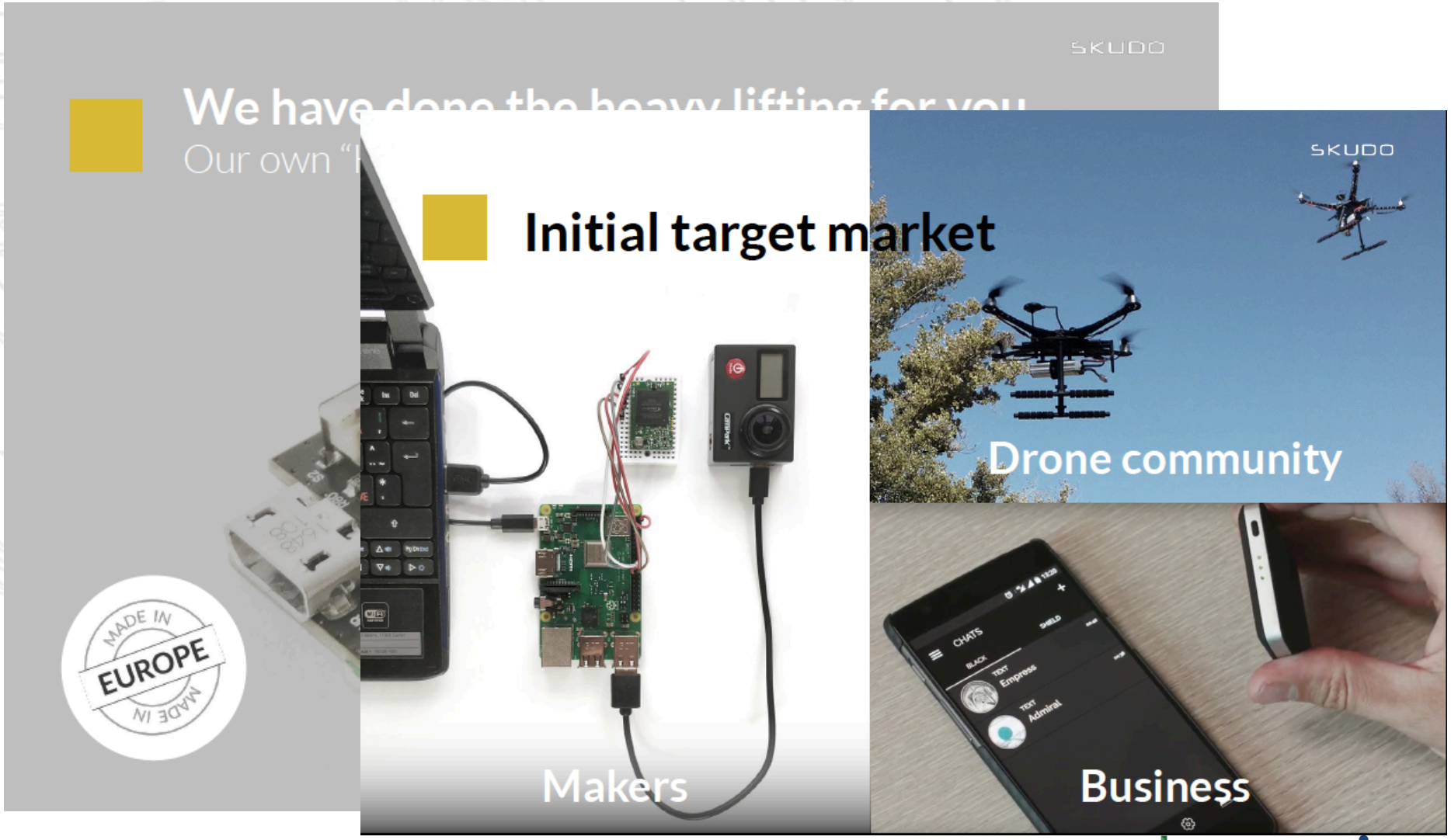




https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf

CyberSecure Robot Development Program – CS by Design

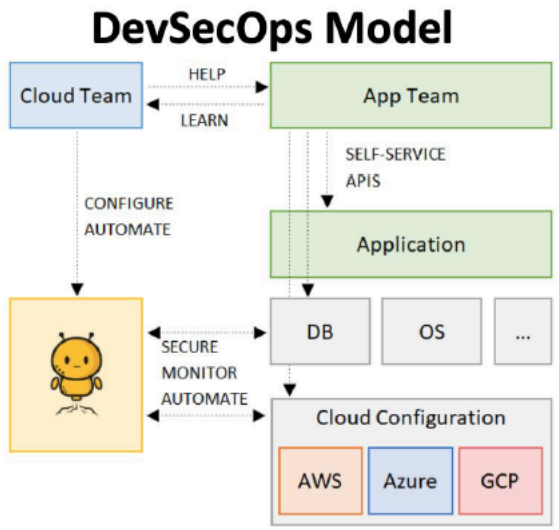
CyberSecurity by Design – Secure Components



CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Reduce Regression testing time©

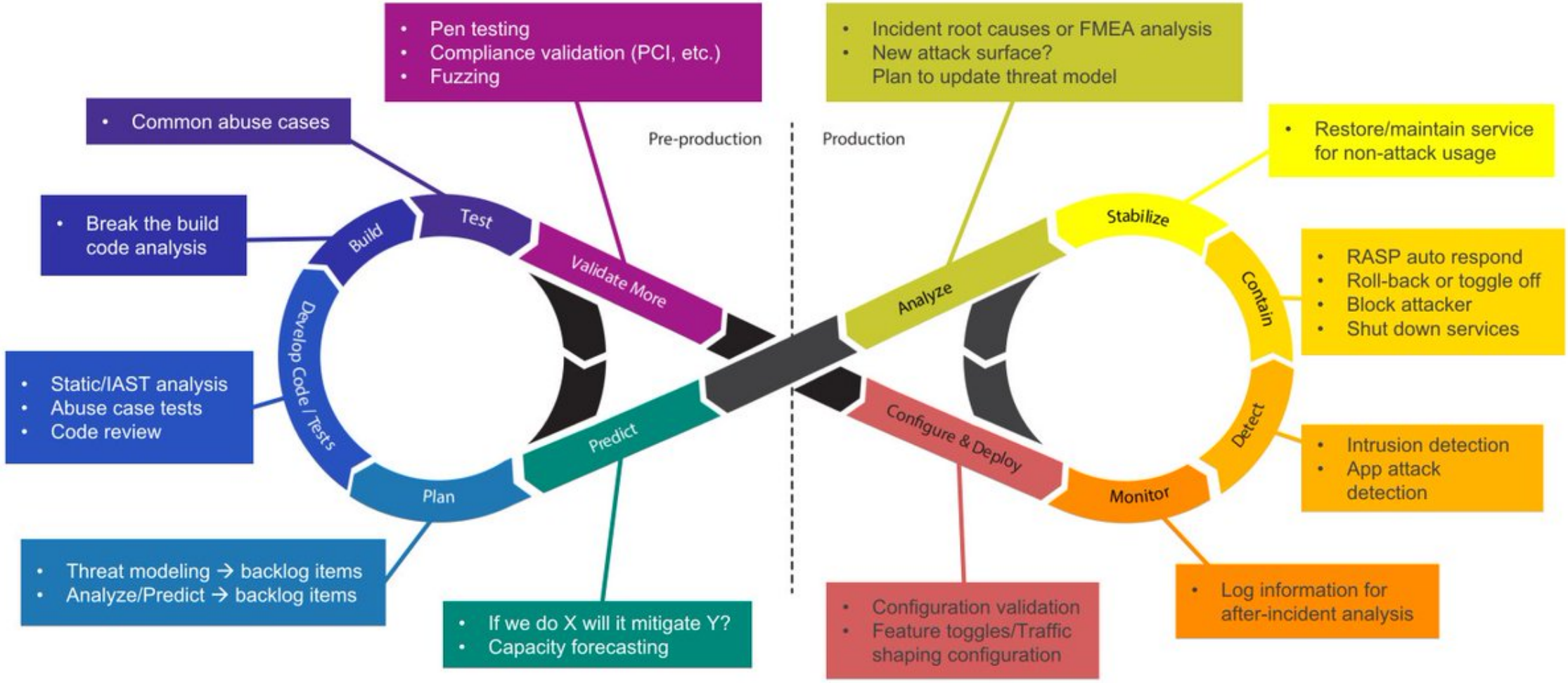
- Architectural risk analysis of the architecture
- Security best practices for the cloud platform
- Continuous vulnerability scanning & penetration test of the application
- Continuous scanning of open source code for security issues
- Continuous scanning of cloud infrastructure for misconfigurations and breaches
- Continuous scanning of source code for security bugs
- Security awareness of staff including developers & operations
- Visibility of security events



Source : LSEC Cloud 2019, Shift Left

CyberSecure Robot Development Program – CS by Design

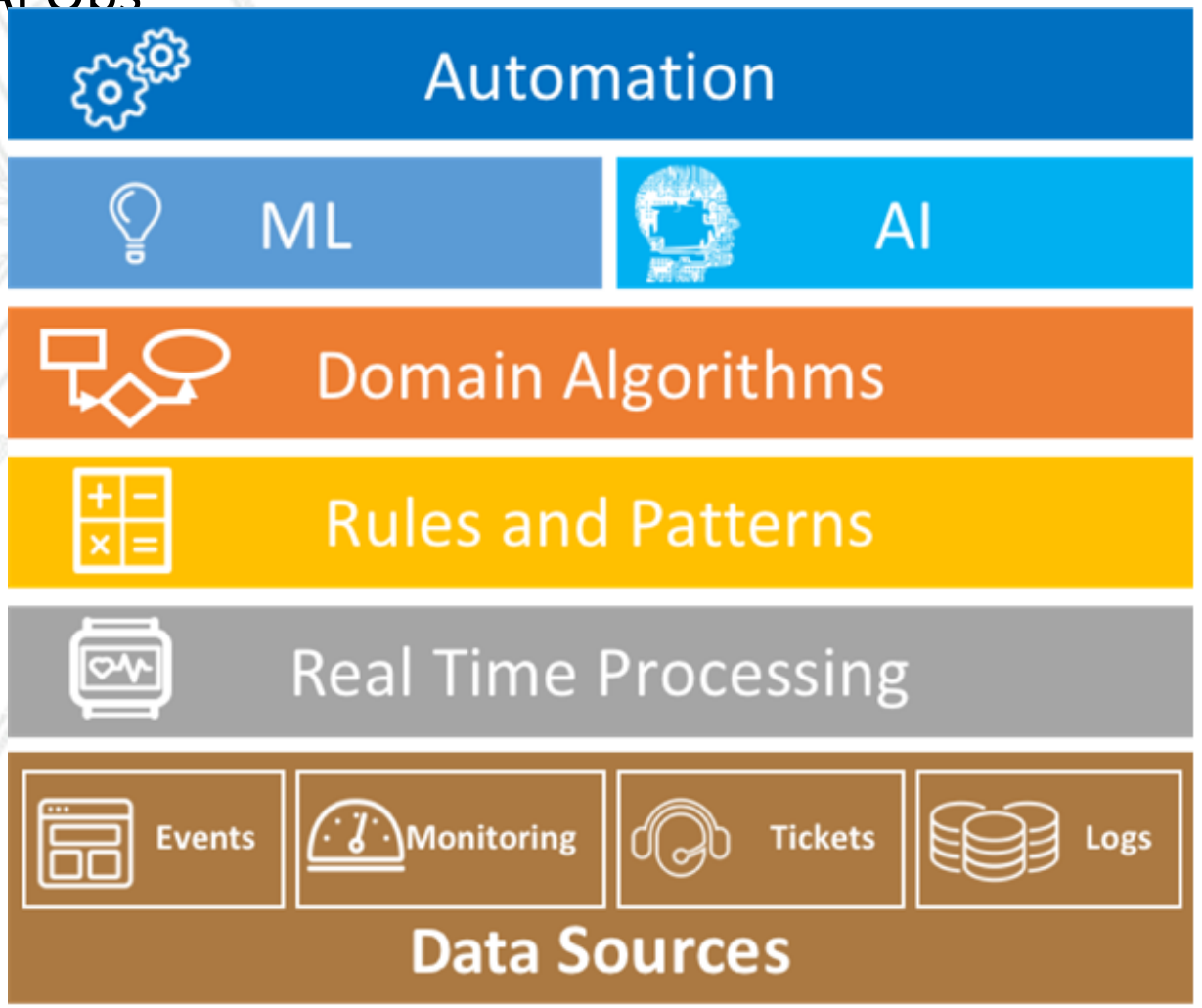
CyberSecurity by Design – DevSecOps



Source : LSEC Cloud 2019, Shift Left

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – DevSecOps to AI Ops



Source : LSEC AI 2019, Shift Left

CyberSecure Robot Development Program – CS by Design

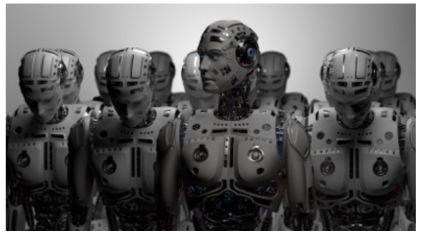
CyberSecurity by Design – AI Challenges

Automation

- DevOps is everywhere
- Increase of using
  - Automation
  - Open Source libraries
  - Containerization
  - Re-use deployment / IaC scripts

New attack vectors

- Taking advantage of automatio
- Open source libraries
- Fast build-deploy
- Containerization
- Complexity and dependencies

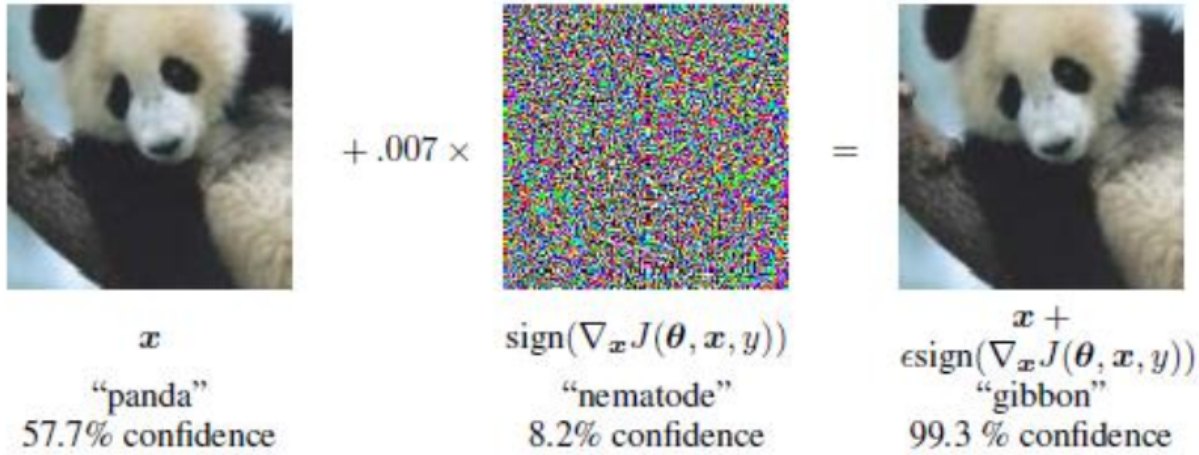


Source : LSEC AI 2019, Shift Left

CyberSecure Robot Development Program – CS by Design

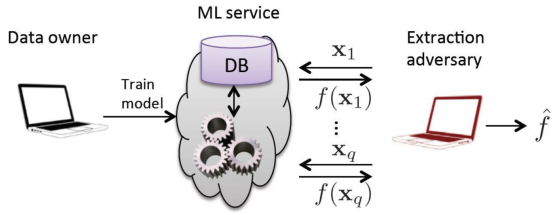
CyberSecurity by Design – AI Cybersecurity Risks

1. Data poisoning
2. Adversarial attacks

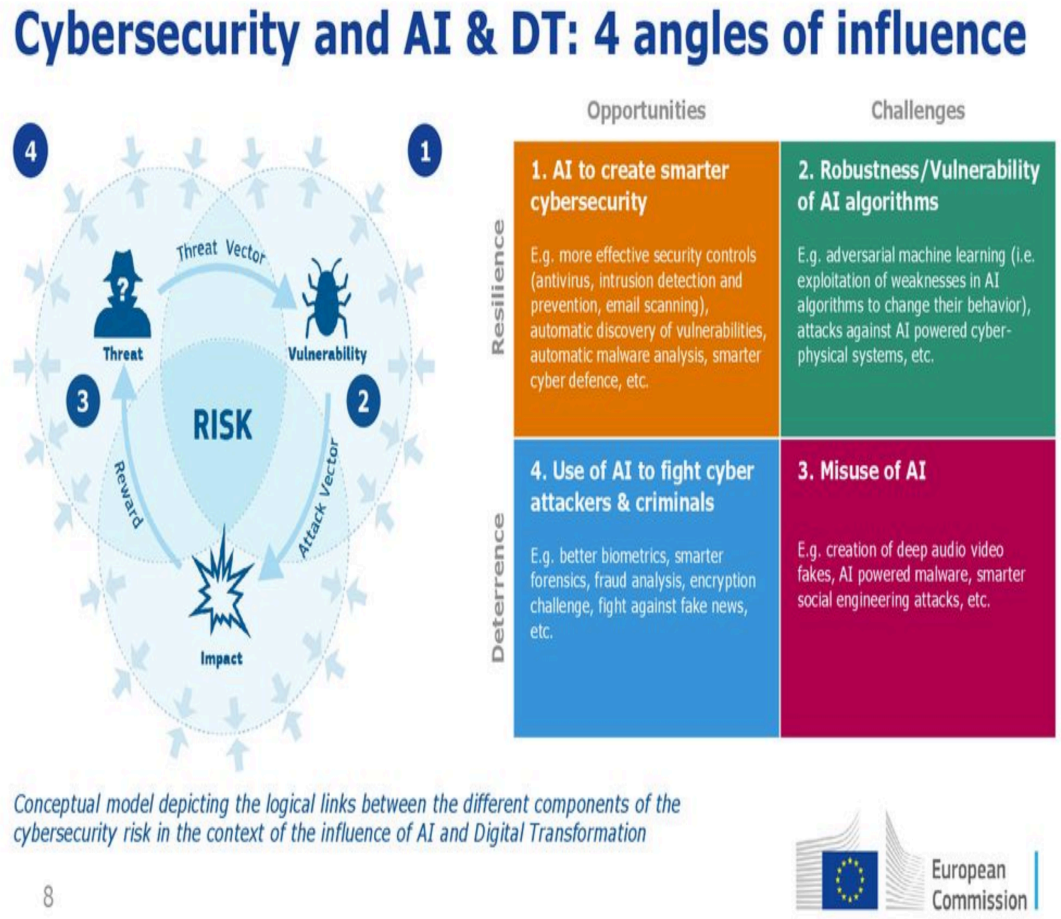


*IBM Research[48] has recently released an open source library called Adversarial Robustness Toolbox ("ART

3. Model stealing (model extraction attack)



4. Video Forgery



Conceptual model depicting the logical links between the different components of the cybersecurity risk in the context of the influence of AI and Digital Transformation

8

European Commission

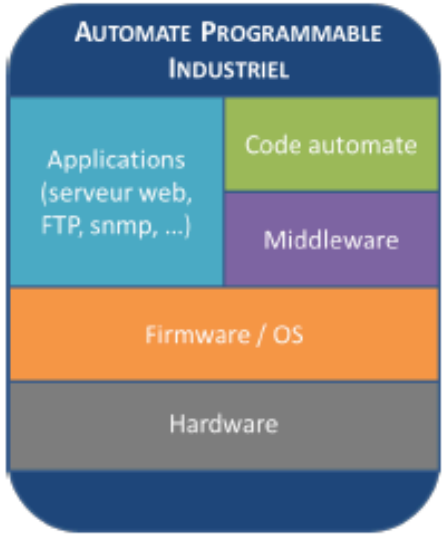
Source: CSSF, 2019

CyberSecure Robot Development Program – CS by Design

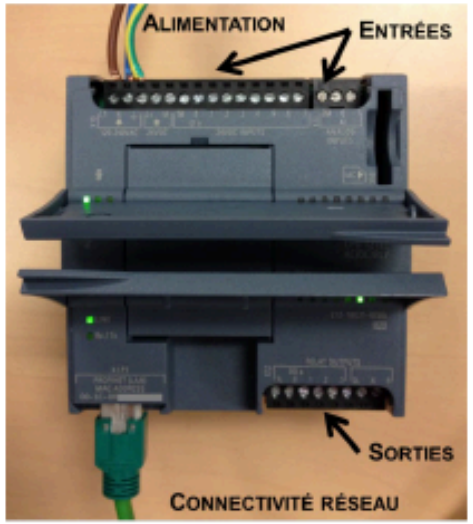
CyberSecurity by Design – use PLC's only if nothing else can be used

- Real-time digital computer used for automation
- Replaces electrical relays
- Lots of analogue or digital inputs & outputs
- Rugged devices (immune to vibration, electrical noise, temperature, dust, …)

What's inside?



Siemens S7-1200

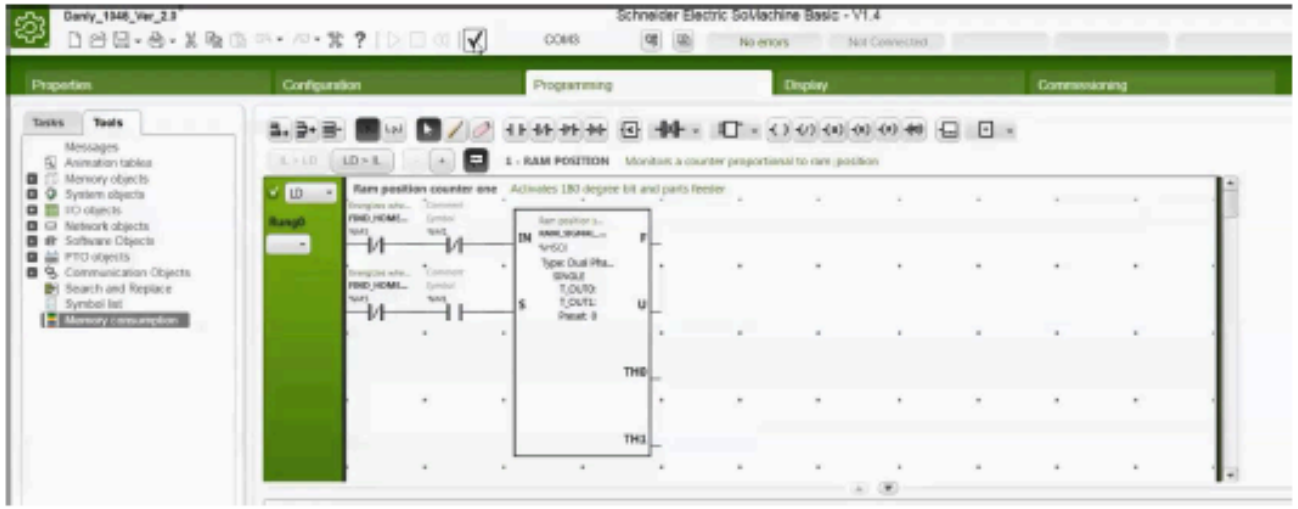


Source : WaveStone Research, 2020

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Use PLC's only if there is no alternative

- SoMachineBasic is the software provided by Schneider Electric to program the entry-level PLCs.
- PLCs used in big plants are usually programmed using Unity Pro, for which there is no free demo version.
- Fortunately, the way this software work is very much the same



PLC programming

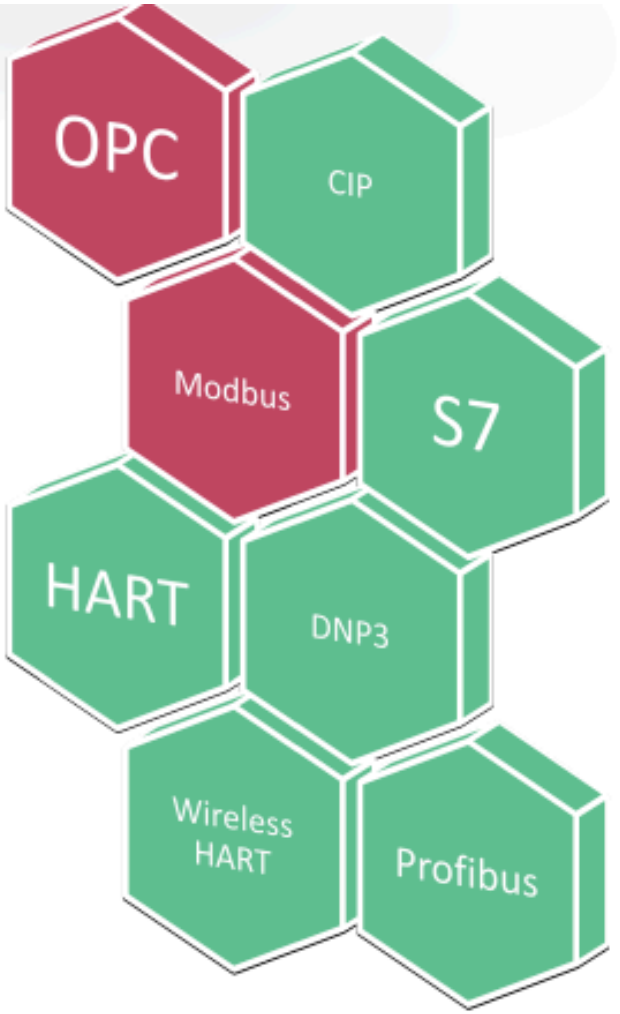
- Create a project
- Define the hardware setup
- Create variables
- Define the program
- Test
- Debug
- Push to PLC
- START

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – PLC's Modbus and OPC inherently insecure

At the beginning, specific protocols on specific **physical layer**
(RS232, RS485, 4-20 current loop)
Some protocols were **adapted to TCP/IP**, like Modbus,
and other were developed to allow interoperability.

ICS devices often use **specific protocols**, some of them are **proprietary**, and some of them are **common standards**
We will hereafter cover the most used ones.



CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – When using PLC's, mind security

- Standard protocol
- Used to exchange data between ICS and Windows devices
- Works on TCP/IP
- Several variants:
  - OPC-DA : Data access, used to gather data from the process control
  - OPC A&E : Alarm & Events
  - OPC HDA : Historical Data Access
  - OPC DX : Data Exchange, allow to exchange data between OPC servers
  - OPC Security
  - OPC XML-DA
  - OPC UA : Unified Architecture, aimed at replacing the others while using a more modern Servi Oriented Architecture.
- Provides authentication and encryption, probably the future of ICS protocols

- Defined in IEC 62541 in 2015
- Designed to replace « DCOM »
- Open and non-hardware specific protocol
- Probably the future of ICS communications

How it works

- Service-oriented architecture (client/server)
- A client can read and edit server nodes, as well as subscribe to them. It is then notified by the server when the node is modified.
- Thanks to the nodes hierarchy and names, it is possible to know what is controlled by the node.
- One server can handle several clients simultaneously.
- The protocol can use « binary/TCP » or « SOAP/HTTP »

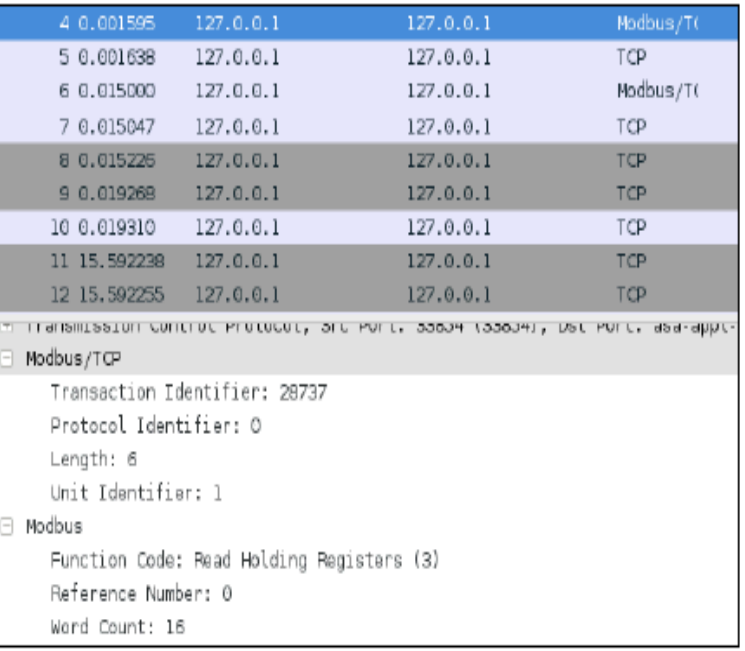
Security

- Several security levels: none, signature, signature and encryption.
- Compatible with X.509 certificates and Kerberos.
- Login/password connection
- Fine grained access rights for each node (read/write).

CyberSecure Robot Development Program – CS by Design

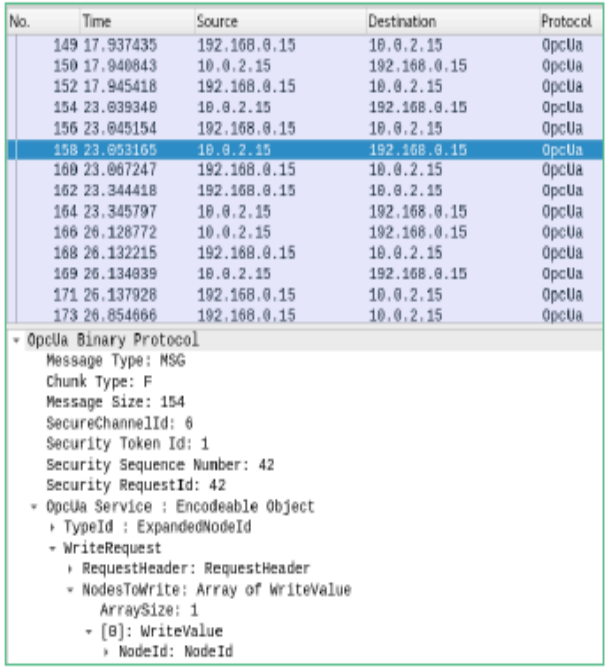
CyberSecurity by Design – network traffic provides insight

- Analyze a Modbus communication with Wireshark
- Wireshark owns by default a Modbus dissector



- Launch Wireshark
- Open « modbus1.pcap »
- Try to understand what's going on
  - Reading request
  - Writing request
  - PLC's answer
- What's the value of register #123 at the end?

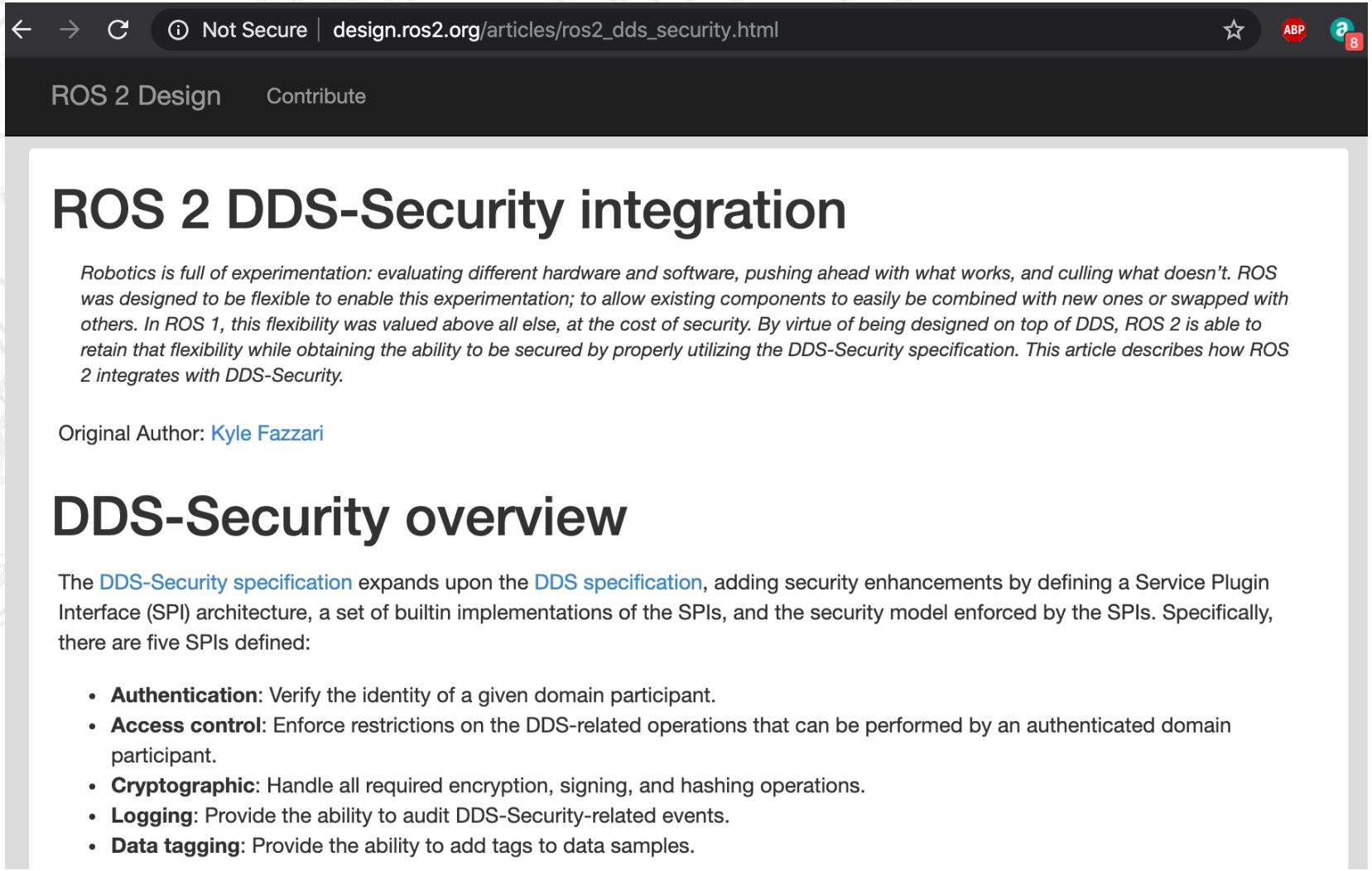
- Analyze an opc-ua communication with Wireshark
- Wireshark owns by default an opc-ua dissector



- Launch Wireshark
- Open « opcua.pcap »
- Try to understand what's going on
  - Browse request
  - Read request
  - Write request
  - Create subscription request
  - Create monitored item request
  - Publish request
- Which node has been changed and what was the value?

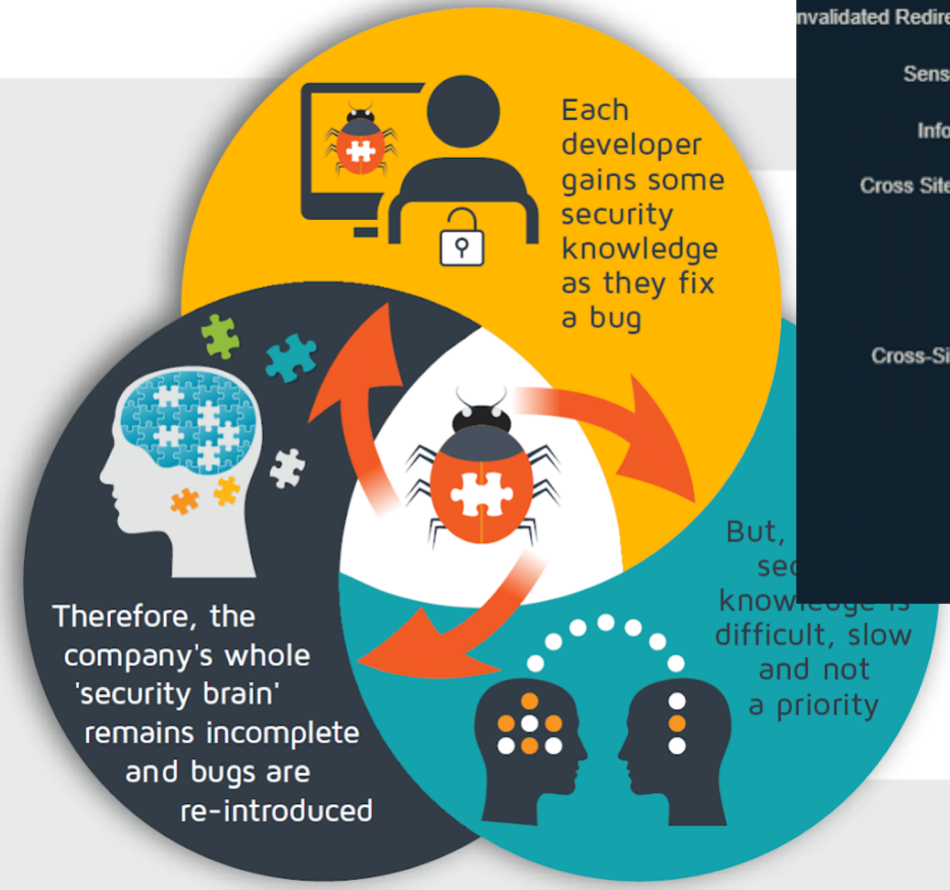
CyberSecure Robot Development Program – CS by Design

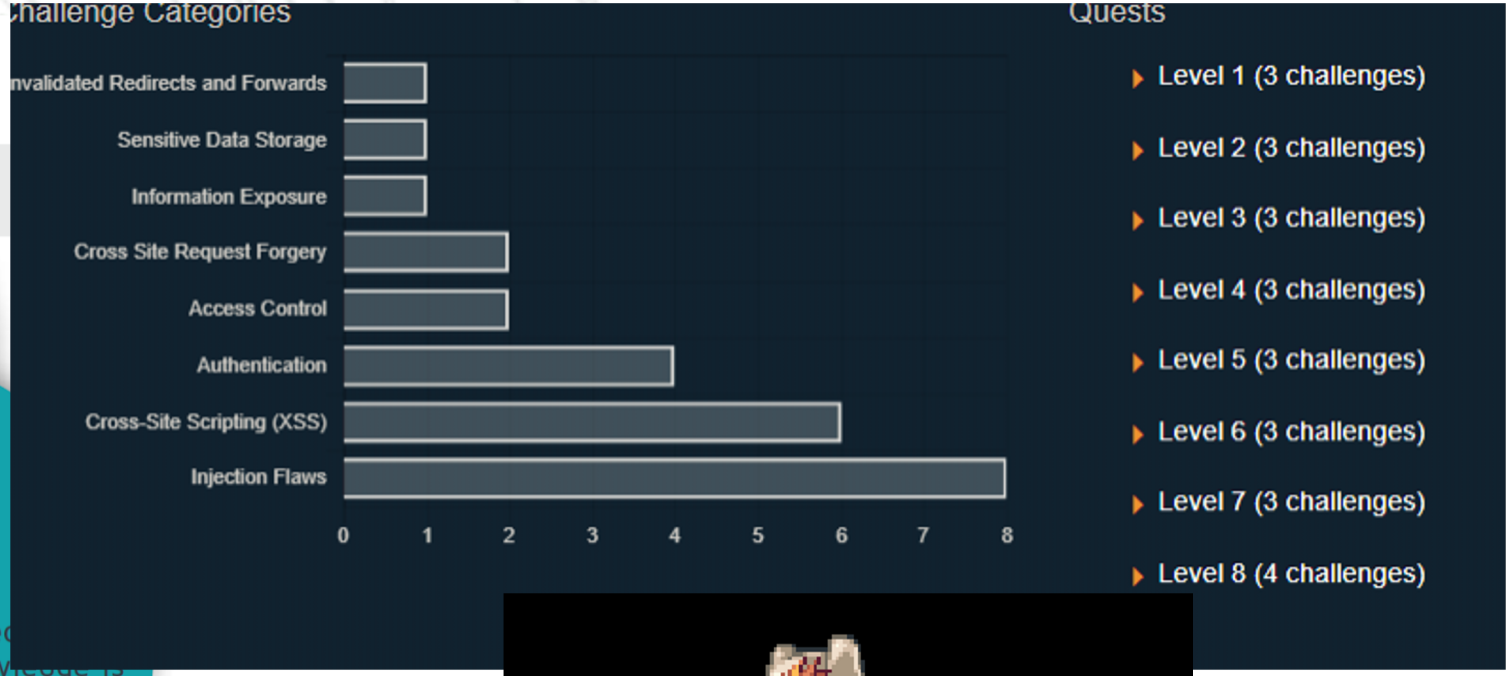
CyberSecurity by Design – Training- (ROS2 Security covered by Viktor)



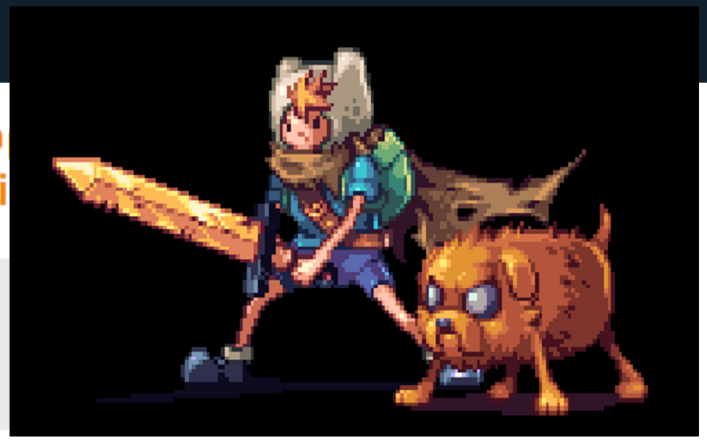
CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Training





→ Today's a
vulnerabi

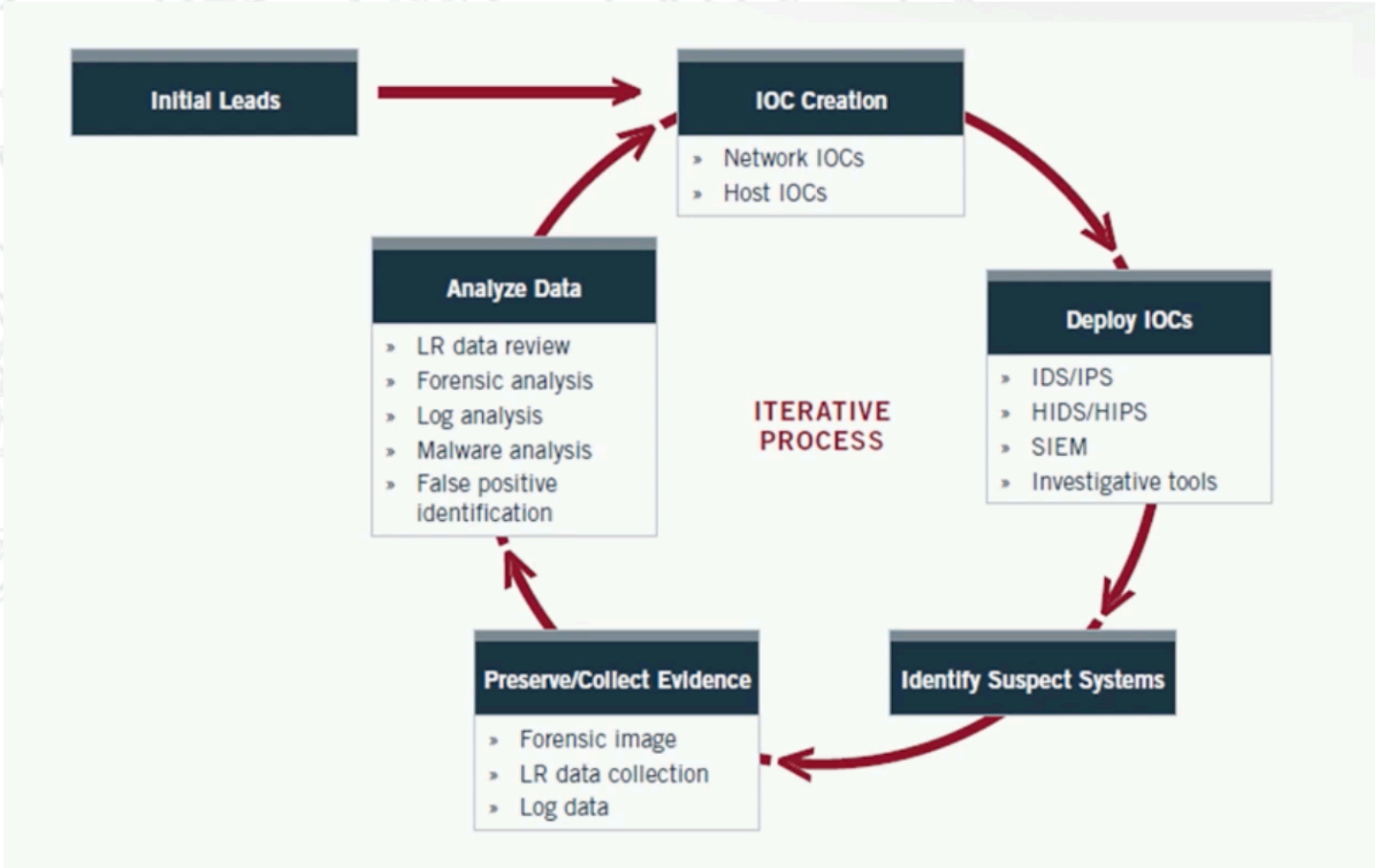


SECURE CODE WARRIOR

TRINITY CSfR CYBERSECURITY FOR ROBOTICS 3IF.be LSEC LEADERS IN SECURITY

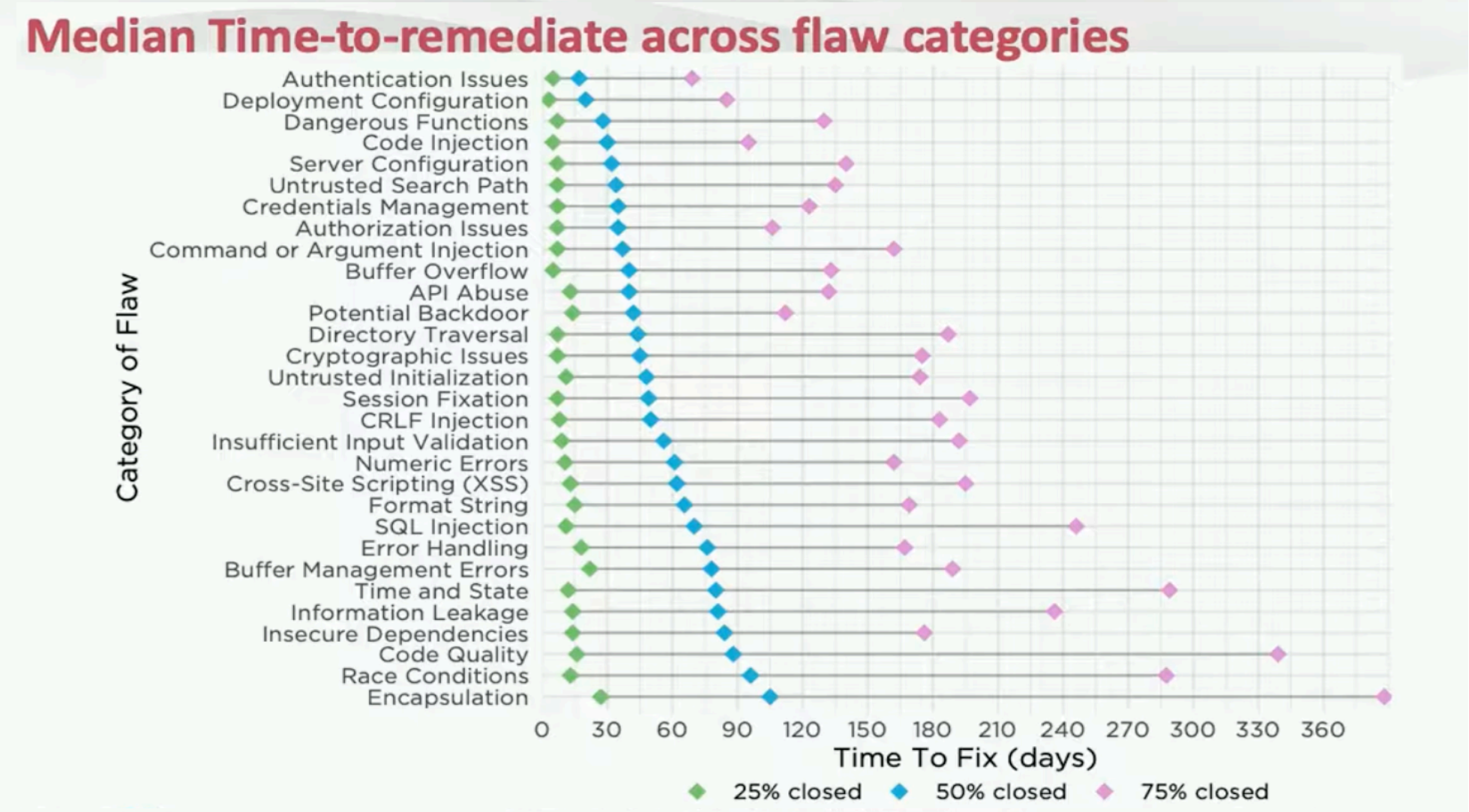
CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Postmarket severity of harm - CVSS – Common Vulnerability



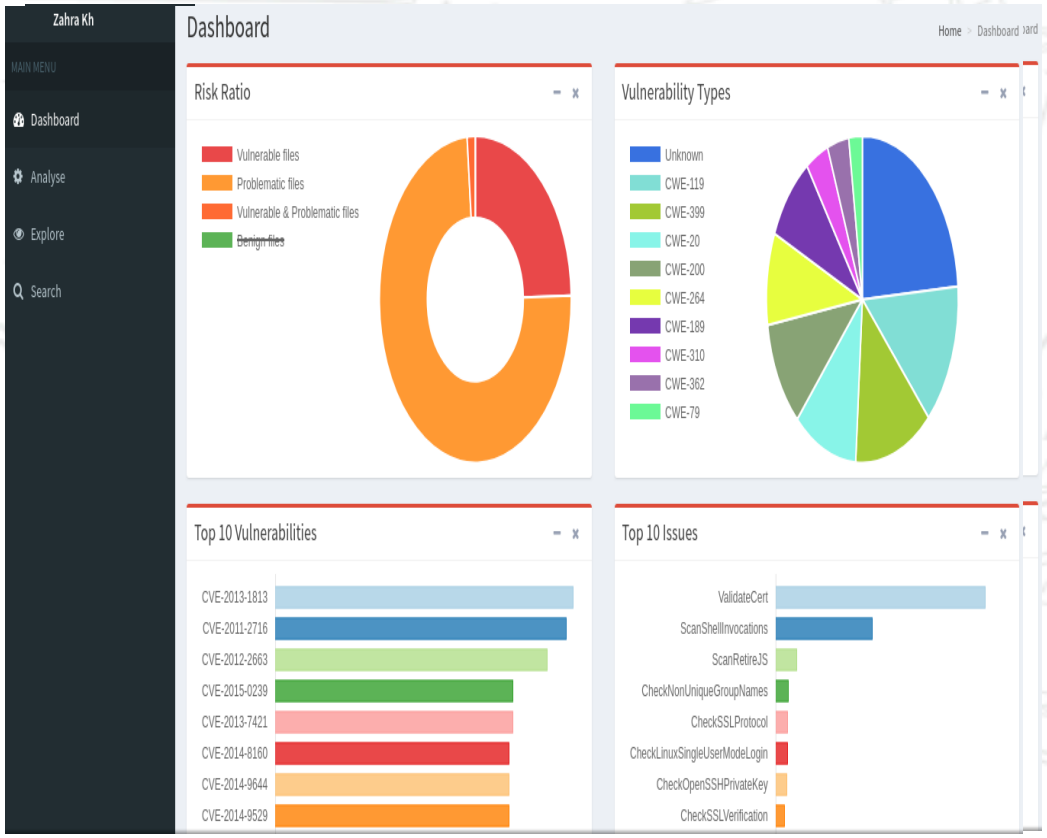
CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Detection of Flaws & Remediation



CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Detection of Flaws – Automated Firmware Analysis



Relies on exposed services over network

Agents cannot be installed on IoT devices

Only detects some issues when they happen

Possibility of harmful impacts / Need the device to be present

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Postmarket severity of harm - CVSS – Common Vulnerability

Robot Vulnerability Database (RVD)

ALIAS ROBOTICS
Robot Cybersecurity

Last updated Mon, 02 Mar 2020 14:37:10 GMT

	Open	Closed	All
Vulnerabilities	vulnerabilities 101	vulnerabilities 12	vulnerabilities 113
Bugs	bugs 346	bugs 193	bugs 537
Others	others 0	others 0	others 0

Vulnerabilities (open)	vuln.critical 23	vuln.high 23	vuln.medium 11	vuln.low 1

▶ **Robot vulnerabilities by robot component**

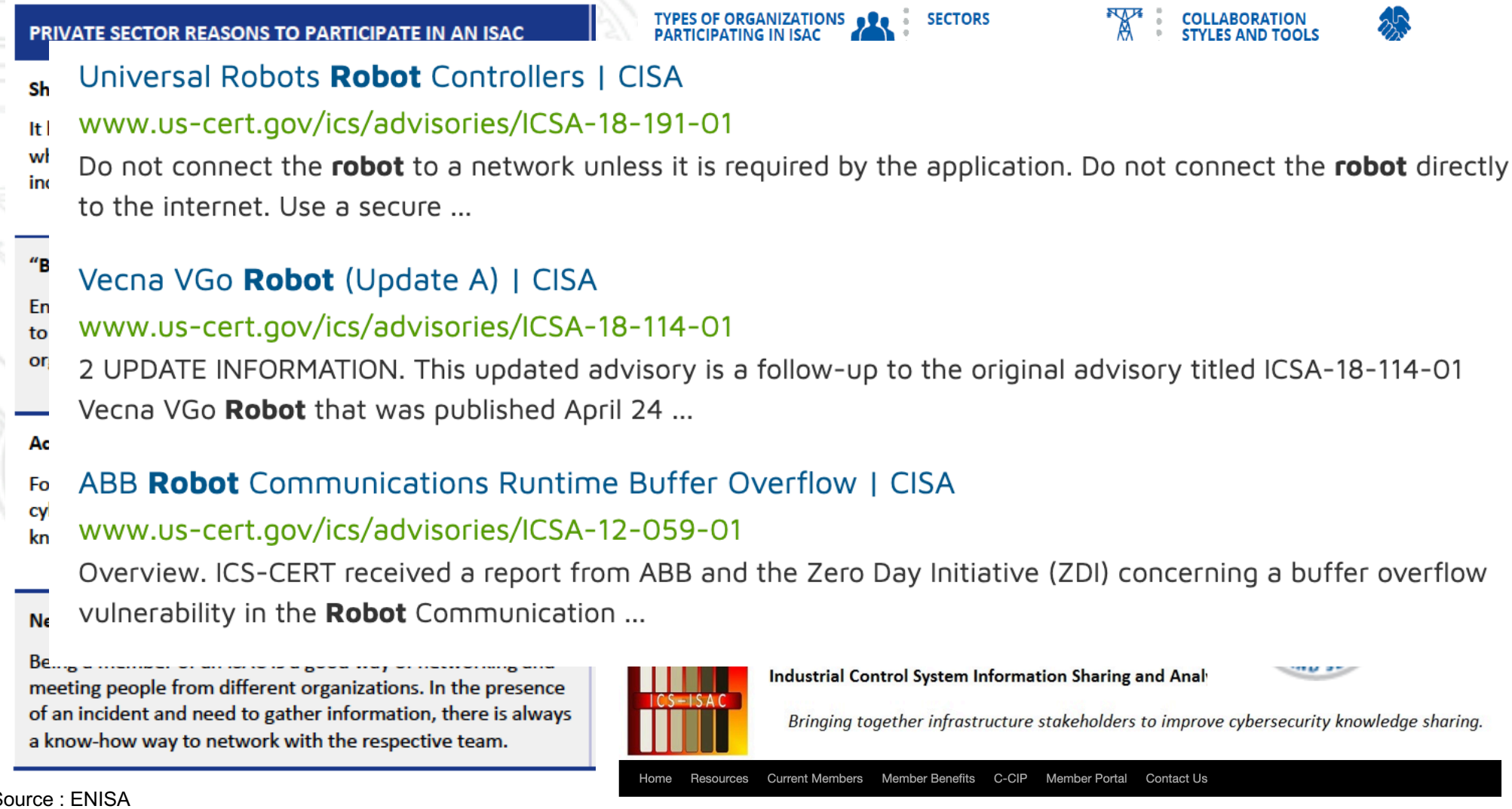
▶ **Robot vulnerabilities by robot**

▶ **Robot vulnerabilities by vendor**

https://github.com/aliasrobotics/RVD

CyberSecure Robot Development Program – CS by Design

CyberSecurity by Design – Postmarket severity of harm - Founding Robotics ISAC

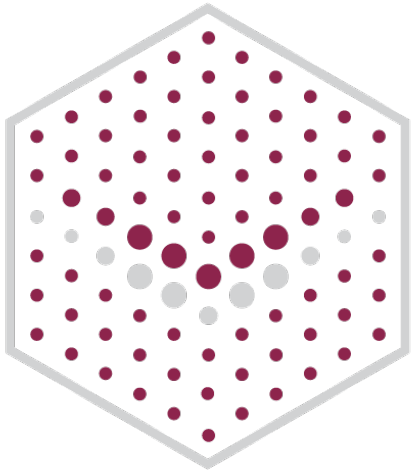


Source : ENISA

Key Learnings

1. Need for a CyberSecurity for Robotics Masterplan
2. All actors in the ecosystem need to be involved and collaborating
3. Other vertical industries and technology domains can provide insights
4. Guidance and materials are available
5. CyberSecurity by Design requires a Program for Manufacturers and Users

6. Join the CSfR community of researchers, industry and users

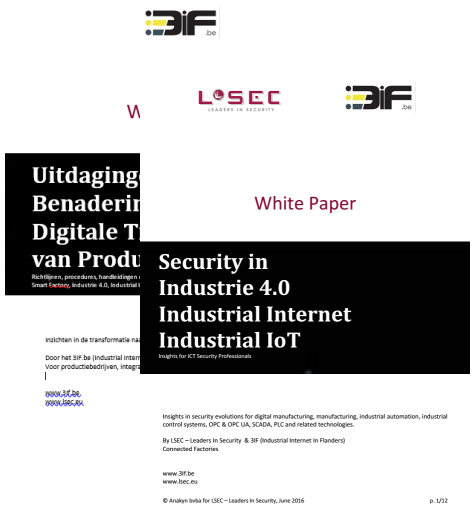


LSEC

LEADERS IN SECURITY

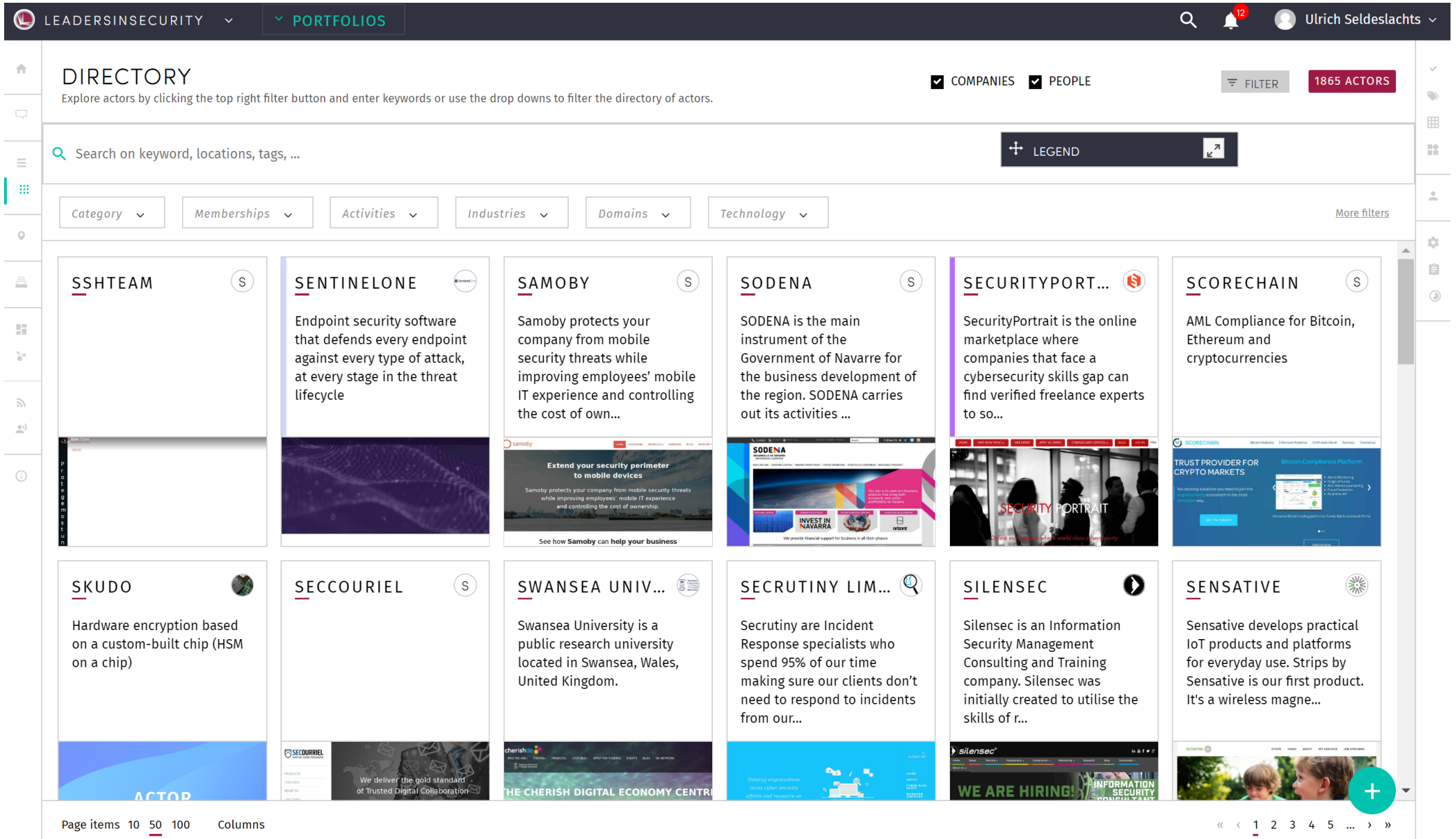
www.lsec.eu

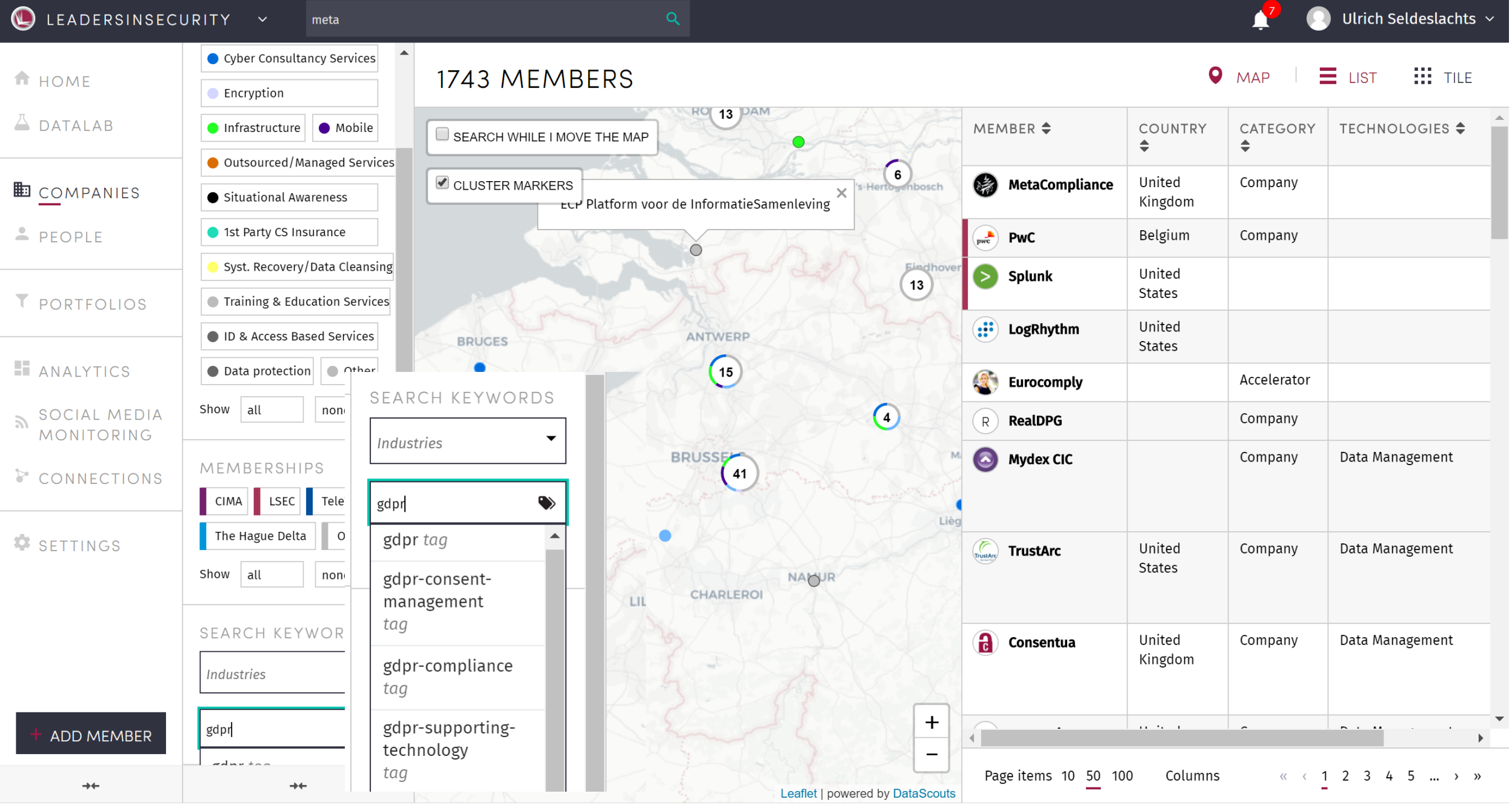
DIGITAL SECURITY CATALYST



LSEC
LEADERS IN SECURITY
www.lsec.eu

MarketIntelligence.Leadersinsecurity.org





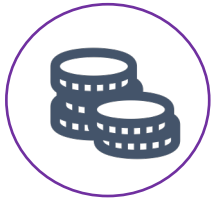
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825196

www.trinityrobotics.eu

DIH TRINITY

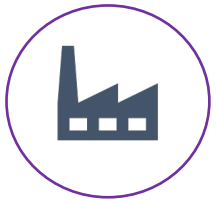
Digital Technologies, Advanced Robotics and increased Cyber-security for Agile Production in Future European Manufacturing Ecosystems

DT-ICT-02-2018 - Robotics - Digital Innovation Hubs (DIH)



Overall budget: ~ € 16 400 000

48 months- January 2019 to December 2022



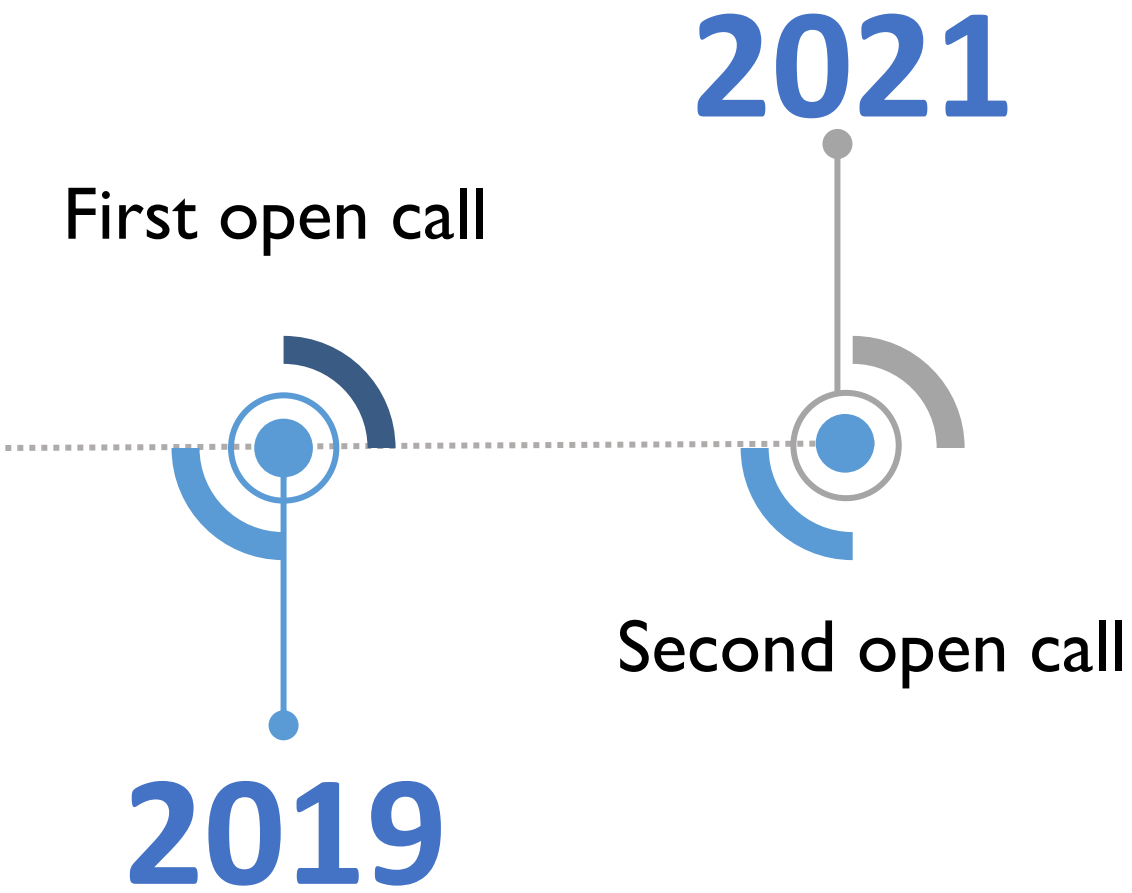
Improve agility & innovation capability of European manufacturing companies (focus on SMEs) through robotics and IoT

Build a network of Digital Innovation Hubs beyond the project life-time

Provide critical mass of use cases to demonstrate new robotic technologies & added-value in different sectors

Create a digital access point to facilitate access to knowledge, collaboration and networking

Open calls



- At least 30 company demonstrators to be funded
- Proof-of-Concepts in industrial environments
- All thematic areas covered
- Calls open for 3 months
- Up to EUR 300,000 funding per demonstrator (70%)
- Total budget 8m€, target budget for 1st Open Call is 4m€

6th 3IF.be international conference

www.3if.be

3IF.be – iotconvention.be

10.06.2020

Industrie 4.0 – Proof International Conference 2019

- 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.

NOT THE END

More information, slides and follow-up

www.lsec.eu

www.3if.be - .eu

Q or C

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