

ECS

EUROPEAN CYBER SECURITY ORGANISATION



FEBRUARY EDITION
AWARENESS CALENDAR

Internet of Things

101 01011

01 110 101 011 010110

01 110 101 011 010110

01 110 10

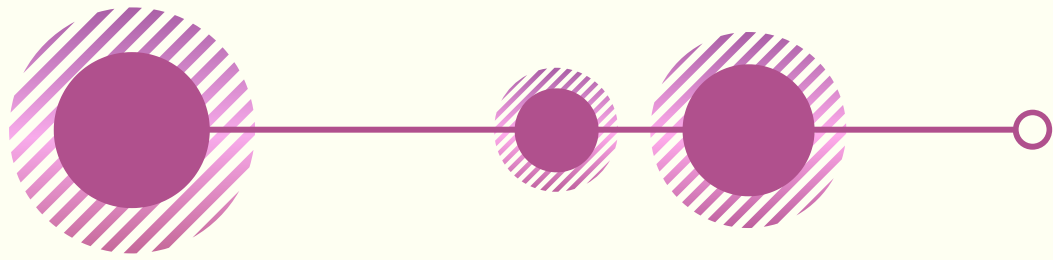
Awareness Calendar **CYBERSECURITY**

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO Members' and Partners' solutions and services in the relevant areas to potential users.



The monthly themes for 2022 are planned as follows:

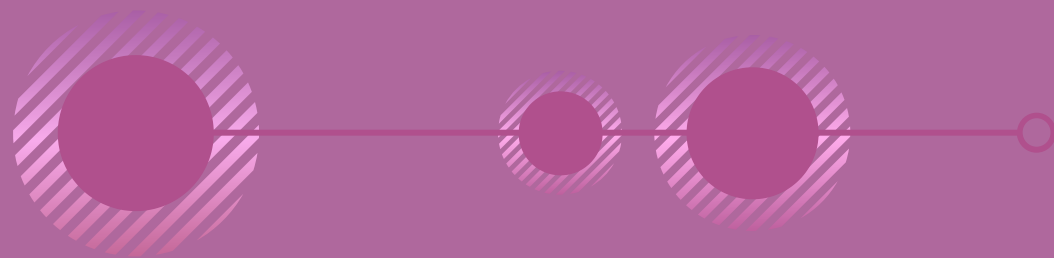
- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management



DID YOU KNOW?

- The European Commission is currently supporting twelve Large-Scale Pilot projects under the focus area Digitising European Industry in Horizon 2020, with a financial contribution of more than €200 million. [READ MORE](#).
- Following the success of Horizon 2020, Horizon Europe will contribute more than €150 billion into R&I under its 2021-22 Calls on 'World Leading Data and Computing Technologies: From Cloud to Edge to IoT for European Data'. Through these calls Horizon Europe will support the paradigm shift to the edge. Focus will be on the development and deployment of next generation computing components, systems and platforms. This will enable the transition to a compute continuum with strong capacities at the edge and far edge in an energy-efficient and trustworthy manner. [READ MORE](#).





RESOURCES FROM OUR MEMBERS

esFirmware - Assess the firmware security of your IoT products



Firmware dictates how IoT devices, and more broadly embedded systems, boot and the startup sequence of memories and other peripherals. At the crossroads of the logical and the physical world, firmware is of particular interest for potential attackers for reverse engineering, hacking or extraction of sensitive assets. Embedded systems firmware security threats can be mitigated with code review, software and hardware countermeasures, logical and physical testings and use of cryptography for instance.

However, how can one ensure that all those security efforts are correctly implemented? Are they effective? Are you using the right security profile? With esFirmware, we automate dynamic binary instrumentation analysis to detect non-security and security related issues via fuzzing, side-channel attacks on data traces as well as simulated fault-injections. The outcomes provide insights and practical data for security assessment and risk management of your IoT devices. [READ MORE.](#)

Addressing the Security of our Interconnected Devices

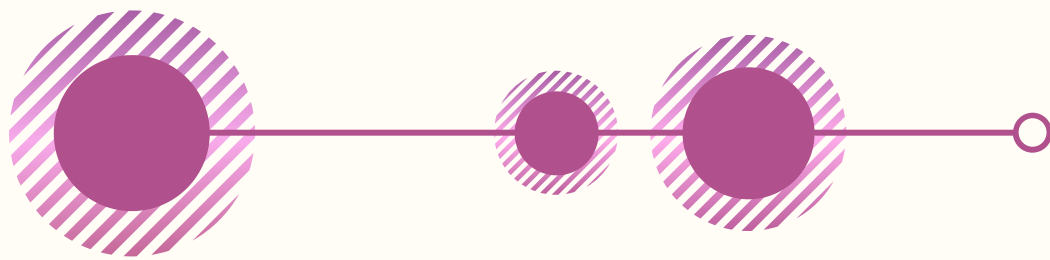


GLOBAL
CYBER
ALLIANCE™

The Internet of Things or IoT is not a new concept, and neither is its security. In the past years, however, this vector of the cybersecurity threat landscape has gained relevance, from a myriad of angles, including policy-making, smart cities, supply chains, critical infrastructures, home office environments, or even consumer goods.

The Global Cyber Alliance, a global nonprofit working to enable a secure and trustworthy Internet, created the AIDE platform and its associated ProxyPot technology to support those efforts back in 2019.

To date, after three years of work and thanks to a network of hundreds of sensors distributed worldwide, we have collected information about literally billions of actual IoT incidents. And our community is using them to change things for real (you can see some examples here and here). Come meet us!



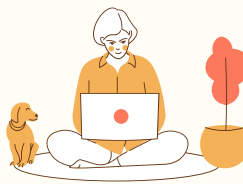
Gadgets@Internet



IoT devices are being increasingly used, but are also a target for cyberattacks that may compromise, with serious consequences, our security.



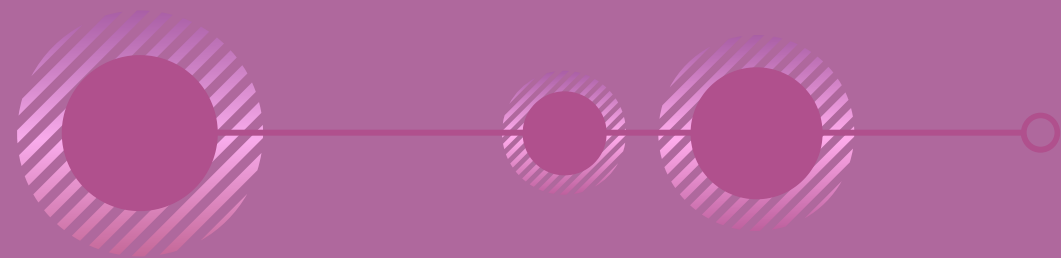
For SMEs: Take a look at the IoT [Temática](#) and at this [Guide](#), with information about: risks in the use of IoT devices, main attack vectors and security measures to reduce the possibility of suffering a security incident.



At home: Set of resources on IoT and the risks of a hyperconnected world. [READ MORE.](#)



For children and educators: Infographic on safety in connected toys with the six keys to take into account before buying or gifting such toys. [READ MORE.](#)



Understanding Security in the IoT Ecosystem: An (ISC)2 Course



The dramatic and rapid growth in the deployment of the Internet of Things (IoT) creates mounting cybersecurity concerns. The skills and knowledge needed to manage those concerns will only grow in demand. This Professional Development Institute course from (ISC)2, which is free to members, provides a broad overview of IoT where learners will be presented with the challenges involved in defining the IoT landscape and how that influences cybersecurity vulnerabilities within the complex, distributed and often unmanaged IoT ecosystem. [READ MORE.](#)





IoT Inspector

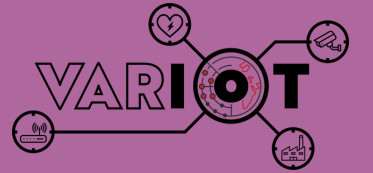
Automate IoT security & compliance to minimise risks and costs

92% of all IoT/OT devices we first analyse contain vulnerabilities, some of them critical. Security and compliance are often not at the forefront of product development and manufacturing. At the same time, cyberattacks on smart devices are becoming more frequent and complex. IoT Inspector is the leading European solution for automated security analysis and compliance checks of IoT firmware. Our clients discover critical vulnerabilities directly during product development and before rollout, while significantly minimising costs and risks.

[READ MORE.](#)


Vulnerability and Attack Repository for IoT

NASK



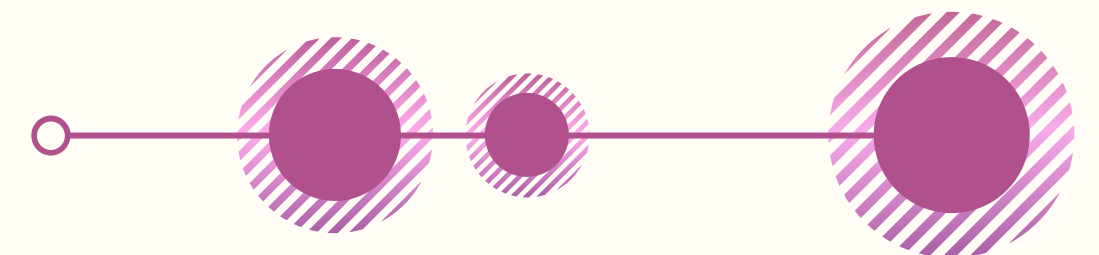
We use IoT devices every day, often without being aware of the risks this usage entails. It is extremely important to raise the awareness of security concerns of these devices. One way to do this is to provide actionable information, for example about vulnerabilities and exploits for a broad audience interested in this topic. Therefore, NASK participates in the VARIoT project, which resulted in the creation of a repository of information on vulnerabilities and exploits in IoT devices. Here you can find the published repository with information aggregated from many sources. Data is also easily accessible through an API, which utilises well-structured JSON and JSON-LD format. Each entry includes sources of information and calculated levels of trust, as well as aggregated links to external sources for further information to be read. You can also find news about security of Internet of Things devices. The repository will be publicly available at data.europa.eu and on the Polish open data portal here.

AIoT: Technical and Ethical Challenges



AIoT is a rather new concept entering into our lives. It has links to various concepts such as Artificial Intelligence (AI), agents, Internet of Things (IoT), things, etc. thus raising both technical and ethical challenges related to the design, development and implementation of AIoT architectures.

Within such a scope and touching a couple of application areas, our work intends to clarify the AIoT concept, present several AIoT architectures and explain how AIoT can be approached in an ethical way. [READ MORE](#).

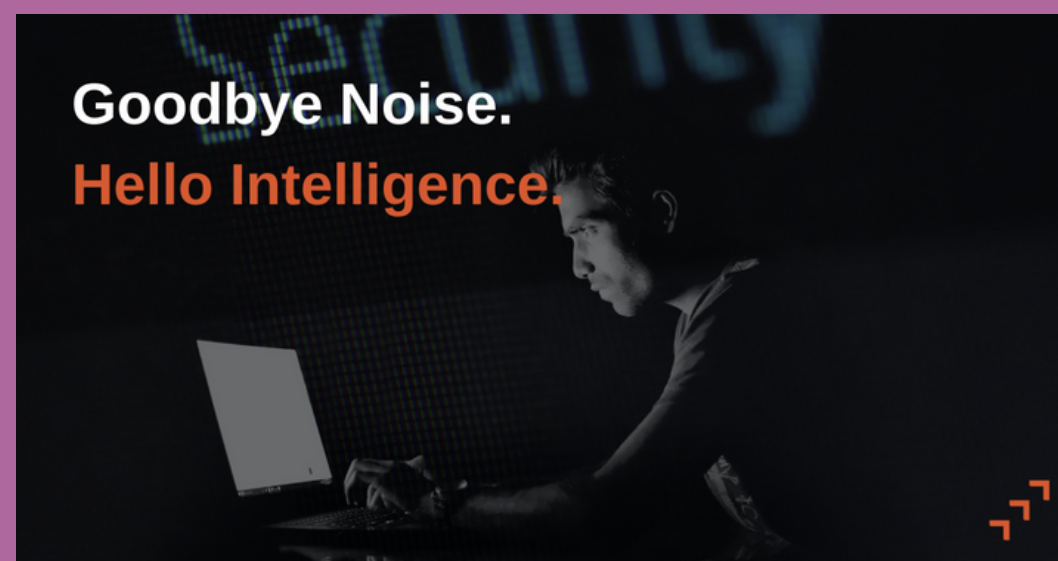




Your Cyber intelligence Partner

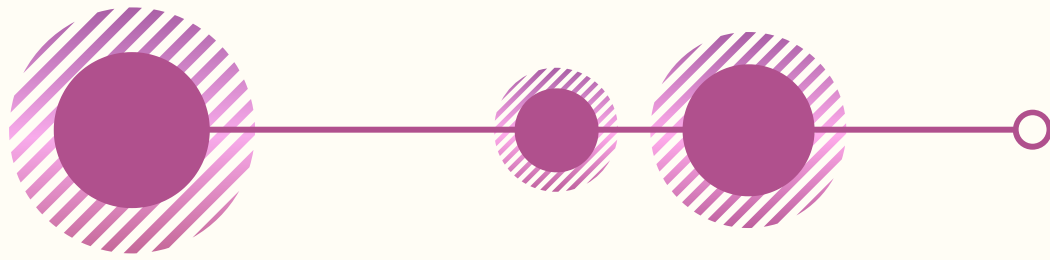
Do you know your IoT regulations?

Regulation plays a key role in sharing IoT security responsibility across all parties. Strong legislation provides equally strong incentives to get IoT security right.



Do you know the regulations in your sector and geography?

It can be complex, we know. We make it our business to understand the regulations. And present them in the way you need to make perfect sense of it. Our knowledge and analysis delivered as you want it. Remove the pain of regulations - call us today.

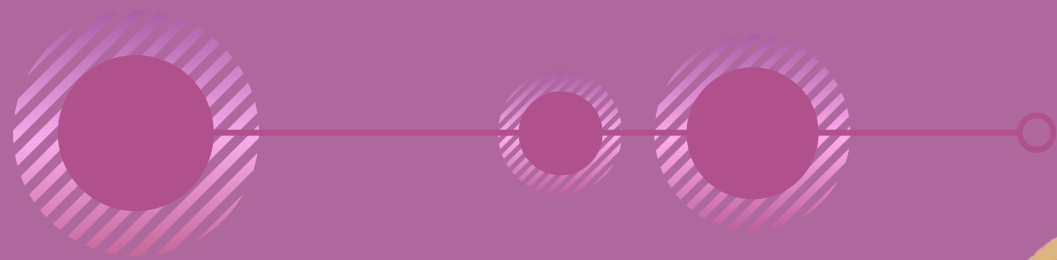


Federated-Learning-Based Anomaly Pattern Detection for IoT Security Attacks



- IoT security is critical for secure IoT devices, IoT platforms and IoT sensors.
- Due to the big amount of collected data, makes IoT networks an open source of data for attackers to perform malicious attacks especially on critical infrastructures
- Due to the growing interest in IoT, there is a wide variety and heterogeneity in standards and implementations if IoT sites even within one Project.
- Moving towards proactive cybersecurity intelligence sharing, there is a huge need for a fast detection and response.

[READ MORE.](#)

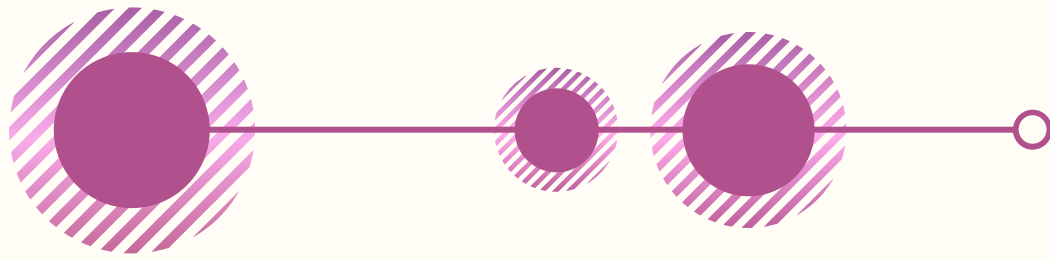


SandGrain

A new European Trust platform for secure authentication of IOT end nodes

SandGrain provides a new European Trust platform for the online secure authentication of any and every electronic part or module of an IoT device, during any moment of its product life cycle. Secure authentication of the IoT device and its constituent parts make the device virtually unhackable and SandGrain elegantly circumvents the “break-one - break all”-syndrome of every IOT device manufacturer. The SandGrain platform also provides an outstanding Secure Firmware Update function eradicating one of the most exploited vulnerabilities of an IOT device.

[READ MORE.](#)



IoT: is it a blessing or a curse?

The principle of IoT is a fantastic idea, but whether it becomes a nightmare for us to deal with or not mainly depends on how well we can keep the whole IoT lifecycle under control. What are the ongoing trends and are we prepared for the rise of the machines? [READ MORE.](#)

**SECURITY
MADEIN.LU**



circl.lu



cases.lu



c3.lu

Cybersecurity Agency for
the Luxembourg Economy
and Municipalities

IoT: What place for cybersecurity?



FACE THE UNPREDICTABLE

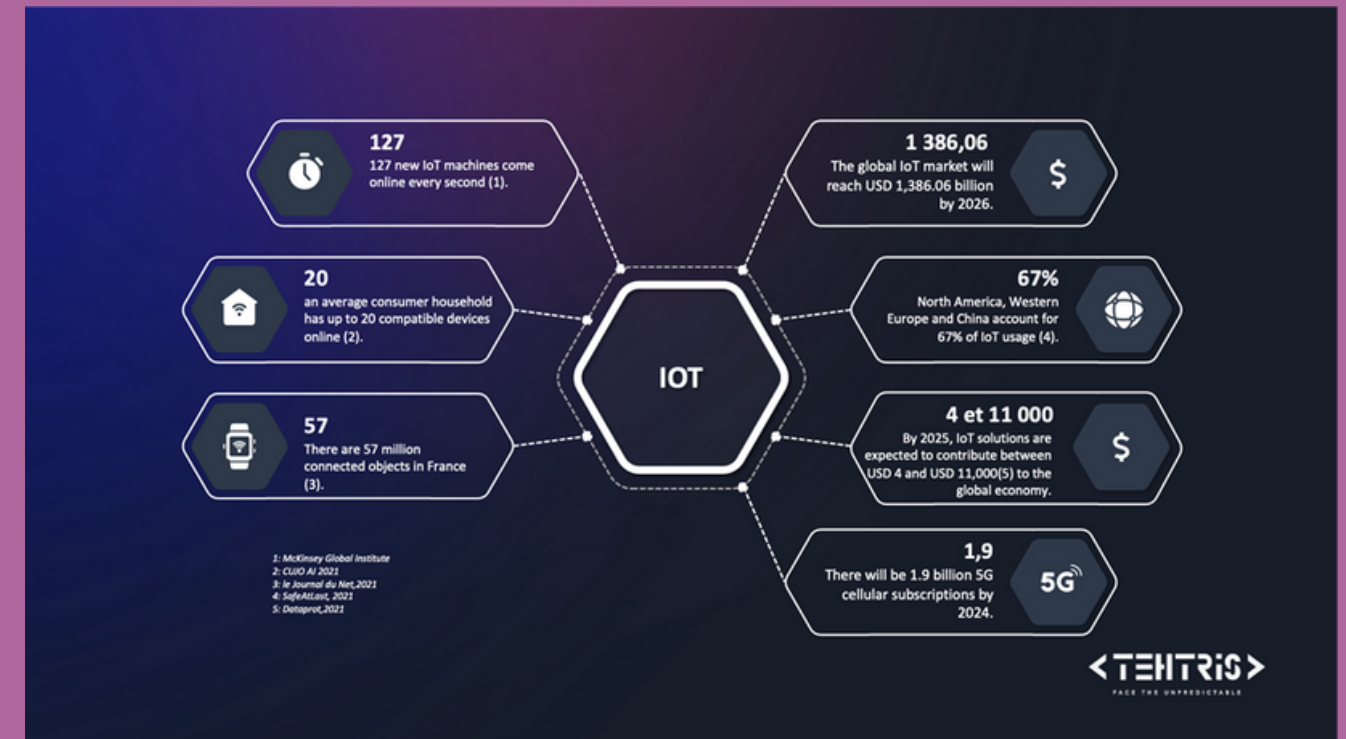
- 75 billion devices will be online by 2035. These new objects are invading our home, our privacy and are becoming not only a threat to the individual but also to the enterprise.
- Respecting the basic protections is key.

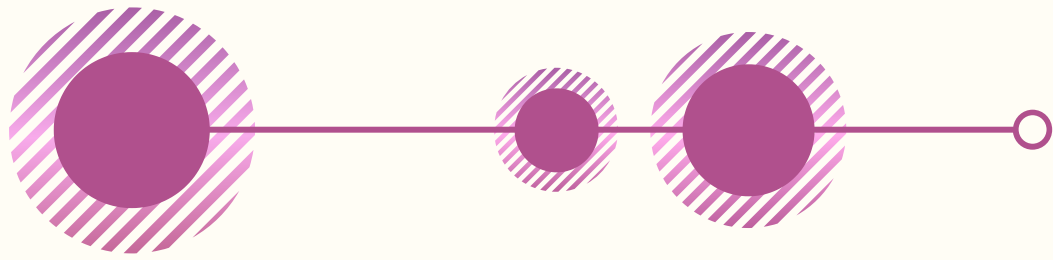
[READ MORE.](#)

IoT: How to protect yourself

- SECURING THE MANUFACTURER'S SIDE
- SECURING THE BUSINESS SIDE
- USER-SIDEESECURITY

[READ MORE.](#)





utimaco®

Utimaco's Connect Gateway and Device Manager

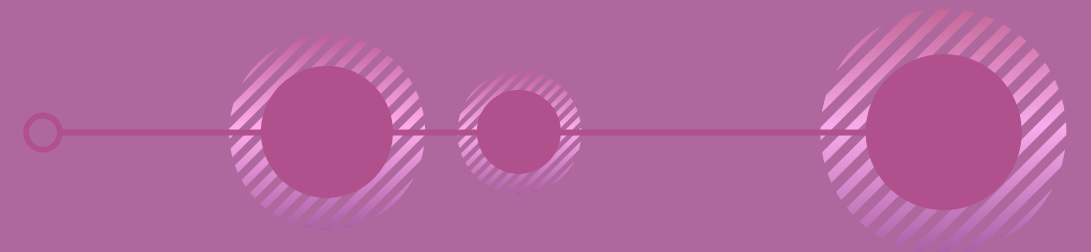
IoT offers more ways for devices to connect to each other and subsequently more opportunities for hackers to intercept. A reliable structure is essential and cyber security for IoT must be built in at the start of the manufacturing process.

With multi-layer security and a highly secure edge computing gateway based on strong hardware protection, as well as centralised device management, Utimaco provides a diverse portfolio solution across various industries for IoT projects to help you save time and costs, whilst minimising your development time and security risks.

Explore Utimaco's [Connect Gateway](#) and [Device Manager](#) to secure and manage your industrial IoT devices.



RESOURCES FROM THE COMMUNITY



10 commandments for IoT

While talking to our numerous industrial customers, ranging from heavy machinery suppliers to workforce tracking and navigation solution providers, I've noticed that my message is evolving into a quite standard form, even to businesses in very different segments and phases. In order to help them to create new products, to optimise existing ones or to just boost overall efficiency with IoT and spimes, I've gathered a few fundamentals to serve as a kind of Ten Commandments of IoT.

[READ MORE.](#)

Critical Importance Of Binary IoT Firmware Analysis & SBoM In Numbers & Facts



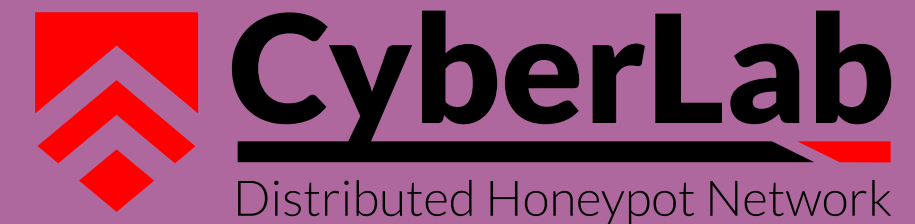
Binary analysis is an in-depth powerful technique to reveal security vulnerabilities in the software components (SBoM) of your IoT device firmware, especially useful when there is no access to source code. 7.9 M vulnerabilities & 3652 distinct CVEs identified in 14.000 firmware files & 178 device types from 215 vendors highlight the critical need to perform binary IoT firmware analysis & identify the software components in your IoT device firmware. Discover more numbers & facts that strengthen the need of binary IoT firmware analysis & SBoM in [Binare's blog post.](#)

Penetration testing and security check of SCADA/ICS systems



SCADA and other IC systems usually control critical manufacturing or state-level infrastructure. Therefore, it is essential to perform regular penetration tests, remediate vulnerabilities, and make these systems as hacker-proof as possible. Carbonsec penetration testers are seriously skilled and experienced professionals with official certifications in SCADA/ICS penetration testing who can help you improve your SCADA/ICS security. [READ MORE.](#)

Exposure of IoT infrastructures to cyber attacks



Digital transformation has led to a rapid increase in the number of cyber threats. By connecting our physical environments to the Internet and storing our most valuable data in external cloud systems, we are preparing an ideal terrain for attackers. Active and passive targets, such as honeypots and internet black holes are instrumental for providing active defense and rapid incident response mechanisms by assessing the threat level and modus operandi of either targeted or untargeted attacks and hacking attempts. CyberLab's distributed honeypot network endeavors to investigate the exposure of modern information and communication infrastructures to cyber risks and to create cyber profiles of both attackers and tools. [READ MORE.](#)

Combination of state of the art technologies to protect IoT architectures



The [H2020 IoTAC project](#) aims to deliver a secure and privacy-friendly IoT architecture that will facilitate the development of more resilient IoT service environments. Our system, comprising of a secure gateway, runtime security applications and cloud-based service platforms, will provide comprehensive protection for service environments of various industry domains. The technology will not only protect new deployments but can also enhance the security level of legacy operations. [View IoTAC's architecture.](#)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952684.

Bad actors have flexed their muscles and showed the industry that practically every device is hackable



Learn IoT-security and memory-corruption basics by hacking IoT devices running on Arm®'s 32-bit processors. Based around two real-world IoT targets that will be emulated, itrainsec course by Maria Markstedter (CEO, Azeria Labs) gets students to learn the process of building and debugging a memory-corruption exploit from scratch, bypassing exploit mitigations such as NX and ASLR along the way. Learn more about the course [here](#).

DNS: Is It Your Organisation's Friend or Foe?



Though the digital transformation in hospitals and other medical institutions comes with extraordinary benefits, the growing use of IoT devices also creates tradeoffs. One major drawback is that digital products and services provide an entry point for attackers, with DNS often being used as a vector for the attack. Find more [here](#).

THANK YOU

for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

 [company/ecso-cyber-security](https://www.linkedin.com/company/ecso-cyber-security)

 [@ecso_eu](https://twitter.com/ecso_eu)

www.ecs-org.eu



secretariat@ecs-org.eu

