ECS
EUROPEAN CYBER SECURITY ORGANISATION

APRIL EDITION
AWARENESS CALENDAR

Artificial Intelligence

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 has proposed a set of actions to boost excellence in AI, and rules to ensure that the technology is trustworthy. The Regulation on a European Approach for Artificial Intelligence and the update of the Coordinated Plan on AI will guarantee the safety and fundamental rights of people and businesses, while strengthening investment and innovation across EU countries. READ MORE.
- The European Commission has opened the second set of calls for proposals of the Digital Europe Programme. This funding will see an investment of over €249 million in several areas: data spaces, European blockchain infrastructure, training courses for advanced digital skills, digital solutions for better government services, projects piloting the use of artificial intelligence (AI) to fight crime, and AI testing facilities. READ MORE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

How will Artificial Intelligence transform our lives?

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Artificial intelligence is already transforming our lives, and its impact is growing day by day. Customer service, transport, education, media, consumption and health are just a few of the fields where AI has already changed or will soon change.

Over time, companies and governments will be able to offer their citizens similar attention: specific and distinctive treatment adapted to each user in all interactions. For this to happen, though, it is not just new technological advancements that are required, but the transformation of infrastructure.

Clearly, data protection and respect for privacy raise many questions, as well as various cybersecurity concerns. The expansion of AI applications should lead to a much needed update of data protection legislation. In April 2022, the Cybersecurity Agency of Catalonia is publishing an article and an infographic on AI, addressing its many advantages and possible issues, and assessing the cybersecurity risks arising from its expansion. READ MORE.

Welcome to information exchange 2.0

The economy is going through a process of unprecedented digital transformation. A key aspect in this process is the mass exploitation of data-driven customer-centric business strategies and models. Security control within organisations make it difficult for data scientists to perform aggregated analyses of multiple data silos, particularly if they are dispersed.

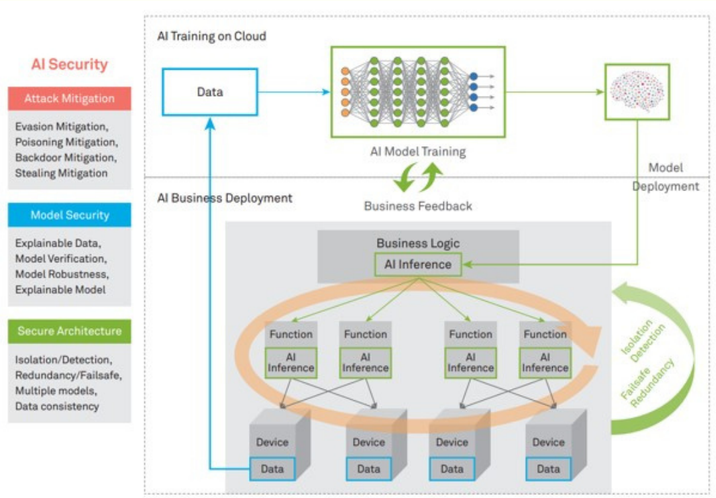
To date it has been necessary to choose between privacy and utility. At GMV we are posing the following question: “Would the problem be solved if instead of sharing data we shared information?”. From that question arose the idea to develop uTile PET (Privacy-Enhancing Technologies), a solution which allows calculations to be made in a safe, private manner using distributed data, without exposing them or moving them out of the organisations. This solution, developed by GMV, uses confidential data to improve machine learning algorithms and analytical models, while at all times meeting organisational requirements, guaranteeing data privacy, in accordance with current legislation. READ MORE.

AI security risks exist not only in theoretical analysis, but also in AI deployments

HUAWEI

To mitigate these AI security risks, AI system design must overcome five security challenges:

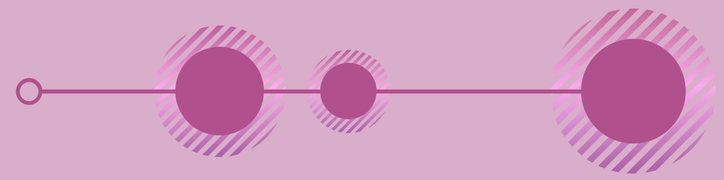
- Software and hardware security
- Data integrity
- Model confidentiality
- Model robustness
- Data privacy



The Huawei Artificial Intelligence for Cyber-Security (AI4Sec) Research Team is responsible for the research and results of AI-based next-generation threat detection capabilities required for Huawei's core security technologies. AI4Sec technical seminars are scheduled to take place every two weeks on Tuesday at 11:00 AM CET/CEST. READ MORE.

OpenUEBA - A systematic approach to learn Behavioural patterns

Data-driven applications are disrupting our actual culture; changing our careers, routines and habits. The Cybersecurity sector is not lagging, being Artificial Intelligence adopted in the nearby 80s as a paradigm to automatise decision making. Even with the great performance of Artificial Intelligence-based technologies, being the core of many actual security tools like IDS, EDRs, Firewalls and more, it is not enough to detect new multilayered attacks on real environments. READ MORE.



INSTITUTO NACIONAL DE CIBERSEGURIDAD

DeepFakes the dark side of AI

Many cybersecurity products use AI to look for signs of possible attacks on our systems and networks, and thus make protection more efficient, but AI is also "useful" to cybercriminals in their search for our security holes and weaknesses. Be careful out there!

For SMEs: The true story of a deep fake of my boss circulating the web. READ MORE.

At home: Deepfakes, how do cybercriminals take advantage of this technology to deceive us? READ MORE.

For children and educators: Methods to protect and teach children about the risks related to deepfakes and artificial intelligence technologies. READ MORE.

Professional Development Courses to Enhance Knowledge of Artificial Intelligence

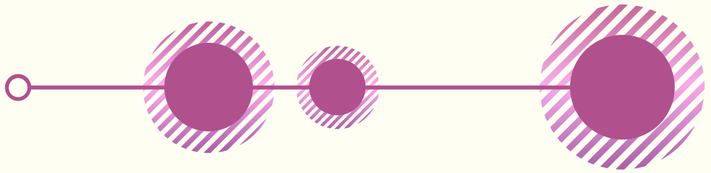
Artificial intelligence (AI) is prevalent in information security professionals' personal and work lives. It continues to evolve and expand and has become an essential component to cyber security. (ISC)² offers several Profession Development Express Learning courses that are free to (ISC)² members and available to non-members for purchase. (ISC)² offers Introduction to Artificial Intelligence where participants will learn terminology related to AI and will be introduced to current practical applications of these technologies. A Security Professional's Guide to AI introduces details of data science in AI, its frameworks, languages and challenges that security professionals face when working with development teams. Both are available in English, Spanish and Japanese. "When Ethics Meets Artificial Intelligence" is available in English and explores the history of AI and related ethical principles. Participants will learn to apply select thought experiments to modern issues and technology. READ MORE.

isep Instituto Superior de Engenharia do Porto

gecad
Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development

AI <-> CS at ISEP/GECAD

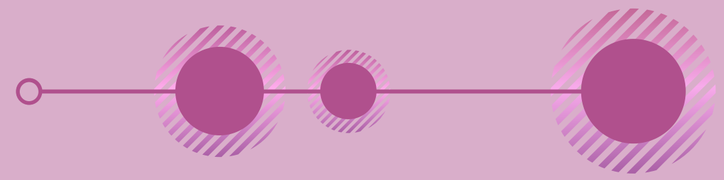
Artificial Intelligence can be a huge help to improve the cybersecurity of multiple systems. Today, AI is being used in several critical sectors. However, AI can be both a blessing and a curse, since it can be used as a protective measure but can also insert several vectors of attack in the systems. Therefore, it is important not only to develop new AI techniques to improve the cybersecurity of the systems (AI for Cybersecurity) but also ensure that these new intelligent techniques are robust and do not compromise the privacy and security of the systems (Security of AI). We work in both fronts, developing robust and secure AI techniques that improve the security of critical systems. READ MORE.



Bürokratt

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Bürokratt is the vision of how digital public services should work in the age of artificial intelligence (AI). Bürokratt will be an interoperable network of AI applications, which enable citizens to use public services with virtual assistants through voice-based interaction. Bürokratt is not just an IT project to create an Estonian state virtual assistant, i.e. an user interface - although this may be necessary as an intermediate step. Instead, Bürokratt will, in the future, allow a person to get everything they need from one device and through a virtual assistant in one communication session. Bürokratt is thus an interoperable network of public and private sector AI solutions, which from the user's point of view, act as a single channel for public services and information. READ MORE.



SECURITY MADEIN.LU

Cybersecurity Agency for the Luxembourg Economy and Municipalities

circl.lu cases.lu c3.lu

Artificial Intelligence

The next wave of digitalisation: AI. Can we surf this digital wave, or will it be the ‘big reset’ that throws us back to the Middle Ages?

There is a massive potential in using Artificial Intelligence, and its areas of application are almost inexhaustible. Integrating AI into cybersecurity systems is not an easy task. Business leaders need to see the challenges of deployment and push to develop solutions that increase the effectiveness of security programs while being ethical and protecting privacy. READ MORE.

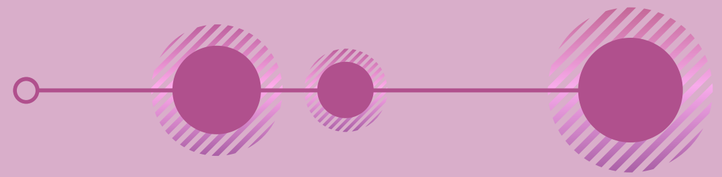
Protected: Why is AI via UEBA transforming cybersecurity?

TEHTRIS
FACE THE UNPREDICTABLE

With the explosion of increasingly fast and complex attacks, defenders must be more resourceful in implementing the countermeasures necessary to fight back, but which ones? One possible answer lies in user behavioural analysis tools.

Endpoint Detection & Response (EDR) and XDR are tools based on Artificial Intelligence and behavioural analysis. UBA for “User Behavior Analytics“, which has been around for a few years, should be part of the detection arsenal of cybersecurity teams.

What is its usefulness and its necessity? And how does it work? How can behavioural analysis interface effectively with existing tools such as SIEM or XDR technology? READ MORE.

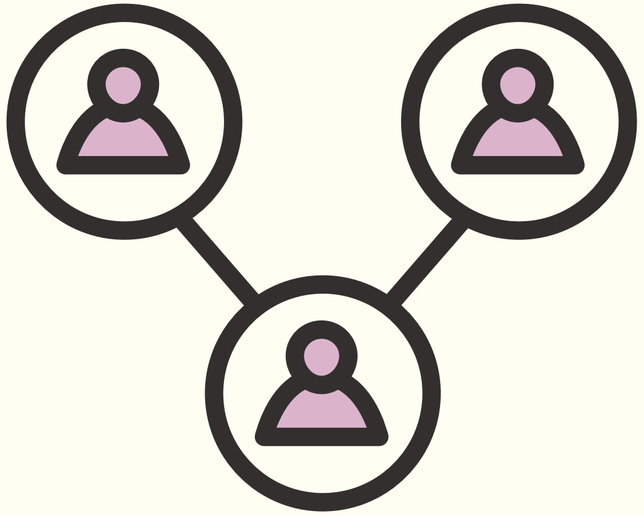


Merging Software Development with AI: A way of looking at the future of AI

Looking ahead into the future, it is likely that we will no longer be satisfied with AI providing decision-making guidance to humans based on commands. Much like we want autonomous vehicles to be aware of the surrounding world, we may want computers to be aware of the world, to save us providing them with explicit instructions, as we do today. That is, we provide commands without the computer being able to relate and make sense, in a cumulative way, of all the commands and data provided. Out of the initiatives that can make computing more effective, is covering the ground to emulate the amount of varied information that humans can process. To this end, the EU, in generating of rules and the legislation regarding AI, needs to build on the broader assumption that as AI evolves, needs for new development will arise. READ MORE.

Cybersecurity and Machine Learning Supporting Each Other

WithSecure™, formerly known as F-Secure Business, continues its research efforts in topics connecting cybersecurity and machine learning. In SAPPAN (has received grant agreement No 833418 under the EU's H2020 research and innovation programme), we have developed several models for detecting anomalous events in endpoints. To increase the reliability of detections reported by the models and to support security analysts in handling those detections, we have experimented with combining detected anomalies in so-called provenance graphs. Our initial approach is presented here. WithSecure has been building its expertise and capabilities in the security of the machine learning domain. As part of our activities in SPATIAL (grant agreement No 101021808 under the EU's H2020 programme), we designed a security self-assessment questionnaire for machine learning-based systems. The questionnaire aims to help organisations assess their posture in security of machine learning and to let WithSecure better understand real-world machine learning security challenges.



RESOURCES FROM THE COMMUNITY

Health, a priority field for the application of artificial intelligence

Kaila has just published an article where we analyse the development of this topic in the EU and also we have detected that the health sector is the area with most funded projects. READ MORE.

Why Organisations Need Automated Threat Intelligence

Automation not only improves the accuracy of threat intelligence, and eliminates mistakes, it is far faster than any human intervention, ensuring the relevant information is sent to those who need to know as quickly as possible. Learn from itrainsec course how to decide whether Machine Learning is an adequate solution for every stage of the threat-intel workflow and, if so, develop an intuition as to which algorithms within ML help us most. READ MORE.

Providing centralised monitoring of cyber, physical and cyber-physical security systems with a SIEM

The Industry 4.0 concept with its ongoing process of digitalisation and automation has completely changed the nature of industrial enterprises, introducing new challenges and extending the so-called “attack surface”. Find out how a SIEM system can help industrial organisations to timely spot suspicious activity and recognise cyber-attacks faster. READ MORE.

Health, a priority field for the application of artificial intelligence

Artificial Intelligence can be used in multiple fields in cybersecurity. As an Extended Detection and Response solution, SEKOIA.IO leverages AI to deliver or optimise some features. The best illustration is the alert prediction that can:

- Detect intrusion with network connections out of classical working hours
- Detect exfiltration with huge download or upload from sensitive servers
- Detect cryptominers on extensive CPU activity on several resources. READ MORE.

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

www.ecs-org.eu

@ecso_eu

secretariat@ecs-org.eu