CYBERSECURITY AWARENESS CALENDAR 2023

SEPTEMBER EDITION:
CYBERSECURITY RESEARCHER
Based on ENISA’s European Cybersecurity Skills Framework (ECSF), this calendar will feature a different skill each month. ECSO aims to spread awareness of key aspects of cybersecurity and showcase ECSO Members and cybersecurity community’s solutions and services.

The monthly themes for 2023 are planned as follows:

January – Chief Information Security Officer
February – Cyber incident Responder
March – Cyber Legal, Policy and Compliance Officer
April – Cyber Threat Intelligence Specialist
May – Cybersecurity Architect
June – Cybersecurity Auditor
July – Cybersecurity Educator
August – Cybersecurity Implementer
September – Cybersecurity Researcher
October – Cybersecurity Risk Manager
November – Digital Forensics Investigator
December – Penetration Tester
Did you know?

1. A cybersecurity researcher conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity. More HERE.

2. Some alternative job titles for “Cybersecurity researcher” are: Cybersecurity Research Engineer, Chief Research Officer (CRO) in cybersecurity, Senior Research Officer in cybersecurity, Research and Development (R&D) Officer in cybersecurity, Scientific Staff in cybersecurity or Research and Innovation Officer/Expert in cybersecurity.

3. ECSO has a Working Group dedicated to research and new technologies which is directly linked to the work done by a Cybersecurity Researchers. This working group has a goal to define the cyber security EU R&I roadmap and vision, establish priorities through a Strategic Research and Innovation Agenda (SRIA) for the H2020 Work Programme and the future Horizon Europe and Digital Europe Programme. Very often, coordinating cybersecurity activities and pilots projects includes working side by side with cybersecurity Researchers who participate on different levels. Together, they assist in the development of innovative cybersecurity-related solutions and contribute towards cutting-edge cybersecurity business ideas, services and solutions through ECSO. More HERE.
Technology innovation: providing prototypes and breakthrough ideas

Technology innovation - it's how we tip disruption in your favour. At our labs, we incubate new concepts and apply the latest technologies to deliver breakthrough solutions for business and society, today. With a massive innovation portfolio of more than 7,400+ patents and patents-pending across Accenture, our team of applied R&D technologists work to prototype and deliver breakthrough ideas that generate new sources of competitive advantage and drive strategic impact for both Accenture and our clients. Each year, we host thousands of innovation workshops and partner with leading clients to transform industries. See how we are shaping the future in our Innovation report.

Our highly specialised R&D groups investigate and apply new technologies to help you deliver breakthrough solutions.

- Artificial Intelligence
- Digital Experiences
- Security
- Future Technologies
- Application Engineering
- Industry X
- Systems & Platforms

Security R&D Group (accenture.com)
Emerging Technologies | Technology Innovation | Accenture Labs
Technology Vision 2023 | Tech Vision (accenture.com)
New types of devices, from body sensors to industrial actuators, are being connected in growing numbers and used in a wide variety of smart applications. How can we control access to the data produced or consumed by these devices? The new IETF standard ACE-OAuth provides a secure and scalable solution for authentication and authorisation of IoT devices, even in the most constrained settings. This is one of the lightweight security standards stemming from a long-term research collaboration, including industry and academia.

Learn more about it HERE.
The Cybersecurity Researcher is one of the cybersecurity profiles defined in the European Cybersecurity framework, required to ensure cybersecurity within organisations.

The main objective of a Cybersecurity Researcher is to identify, understand and mitigate cyber threats to protect organisations, systems and data from cyber attacks.

Exprivia's Cybersecurity Observatory consists of trained and certified Cybersecurity Researchers tasked with analysing cyber attacks, security incidents, and privacy violations.

Exprivia's team of Cybersecurity Researchers provides data collected on attacks, incidents and privacy violations for the benefit of those working in the world of CyberSecurity, from its CyberCrime Observatory that collects data in Italy, Spain, Brazil and Canada. In the Threat Intelligence Report, the Observatory uses public information focusing on the perimeter surveyed by analysing thematic areas relevant to the period in question.

Learn more about it HERE.
Learn new skills and what it’s like to be a Threat Intelligence Analyst! (FOR FREE!)

The Cybersecurity Career Path is part of the Cybersecurity Learning Hub which is an initiative designed to tackle the global cybersecurity skills shortage. Hosted on Trailhead, Salesforce’s learning platform, it provides over 70 free courses with career oriented information, expert interviews and training modules. Take the Threat Intelligence Analyst Trailmix to learn how and what it’s like to identify cybersecurity threats through information collection and threat intelligence. You can also check out other cybersecurity roles and learn vital skills for free whilst you’re there!

Global Cyber Alliance is proud to be a founding partner of the Cybersecurity Learning Hub alongside the World Economic Forum, Salesforce, and Fortinet.
ISC2 Professional Development Opportunities and Cybersecurity Certifications for Cybersecurity Researchers

CISSP certification. The global gold standard in cybersecurity. This certification demonstrates vendor-neutral knowledge to design, implement and manage a best-in-class cybersecurity program in any environment.

Preparing for a Zero Trust Initiative - This course presents foundational principles, threat scenarios, reference architectures and a policy governance framework that can be applied to reduce risk.

SSCP certification - Demonstrates advanced technical skills and knowledge to implement, monitor and administer IT infrastructure.

Implementing and Reviewing SETA Programs - This course reviews strategies for implementing, measuring and reporting SETA program outcomes.

The What, Why, Who and How of Cybersecurity Strategy
This online training addresses creation and implementation of cybersecurity strategy, protecting assets and reducing cyber risk. Learn more about the elements of a strong and successful cybersecurity strategy and why that's important.
i2CAT Cybersecurity and Blockchain Area

Targeting real world problems and generating knowledge and assets for a trusted societal cyber growth and awareness.

Research and innovation working together with two dimensions: the catalan Cybersecurity community in collaboration with the Cybersecurity Agency of Catalonia and the EU Cybersecurity Innovation Lab.

Research topics:

- **Cyber-threat management and response**: Going forward in Security Orchestration, Automation and Response (SOAR) augmented with Security Information and next generation of predictive risk management platforms.
- **RISK Assessment and Management**: Developing new functionalities and business models integrating technologies such as Artificial Intelligence, Robot Process, Automation on Risk assessment and management processes.
- **User-centric security practices and tools**: Exploring and defining new ways to empower users and manage their privacy under sovereign data and identity platforms of the future.

Learn more HERE and HERE.

Technologies:

- Machine Learning Threat Behavior Analytics
- 5G and IOT Security
- Cybersecurity for connected and automated vehicles
- Zero Knowledge Proof

Applications:

- Active Risk-Response Systems
- Next generation SOC/ISAC tools
- Analytics-driven cloud SIEM and Intelligent SOAR
- Digital Identity
KINAITICS: Cyber-kinetic attacks using Artificial Intelligence.

From the ubiquitous use of AI in cyber-physical systems, threat and risk assessments need to be redefined to take into account the interconnection of the cyber and physical worlds and the dual use of AI. That’s one of the most ambitious challenges of researchers nowadays.

Among specific targets, in KINAITICS we have to:
- Evaluate the risk of physical attacks by studying advanced attack exploitation frameworks leveraging AI.
- Define defence strategies in the context of cyber-physical systems security with help of AI.

Specifically on social engineering, we are targeting spear phishing. This kind of malicious email is not distinguishable from the good one with current tools. We are going to investigate how to improve the email assessment with advanced NLP analysis using AI.

This project is funded by the European Union.

Read more HERE.
Resources from the Community
Barikat Cyber Security, a pioneering leader in cybersecurity, is committed to its motto, "Security & Protection for All." Through extensive in-house research and development, Barikat offers cutting-edge solutions to establish a comprehensive security ecosystem. Loddos, the cloud-based DDoS Testing (SaaS) platform, assesses organisations' cyber resilience, while ASMA, the asset management and service detection system, ensures immediate responses to security issues. With internationally acclaimed R&D solutions, Barikat collaborates with stakeholders to enhance digital security standards and counter cyber threats effectively. More HERE.

What It Means to Be a Cybersecurity Researcher: Insights from Industry Experts

In the cybersecurity industry, few skills are as critical as those that cybersecurity researchers possess. They are extremely knowledgeable computer experts who spend their time looking for vulnerabilities in systems and investigating malware. They also analyze malware to understand its capabilities and possible targets, thoroughly documenting any incidents of compromise. No one has a better understanding of the best steps for mitigation of today's threats, and as such, the cybersecurity industry could function without these specialists. This month, we spoke to several cybersecurity researchers, to get their take on the job, its challenges, and rewards. More HERE.
As the digital landscape becomes increasingly complex and interconnected, the demand for individuals who specialise in fortifying the digital world against evolving cyber threats has skyrocketed. This is where cybersecurity researchers come in. With an eye on evolving trends, they customise security to fit the unique needs of various sectors, enhancing cyber resilience and anticipating threats. But while charting their course into the future, they face a set of challenges. More HERE.

Automatic Runtime security for containerised workloads

The research behind Quritis shows that the attack surface is significantly reduced with tailor-made security profiles for a containerised workload. Quritis is building a SaaS service that integrates easily into the developer workflow. Once integrated, it provides automatic and continuous behavioral analysis of their software and generates security profiles used in the operational context. Anomalies and potential deviations can be detected automatically, and the security profile can block exploitation attacks against the containerised workload. More HERE.

Cybersecurity Researchers: Adapting to the Ever-Changing Threat Landscape

As the digital landscape becomes increasingly complex and interconnected, the demand for individuals who specialise in fortifying the digital world against evolving cyber threats has skyrocketed. This is where cybersecurity researchers come in. With an eye on evolving trends, they customise security to fit the unique needs of various sectors, enhancing cyber resilience and anticipating threats. But while charting their course into the future, they face a set of challenges. More HERE.
Thank you for your time!

The Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
Avenue des Arts 46
1000, Brussels

LinkedIn: company/ecs-cyber-security
Twitter: @ecso_eu
Website: www.ecs-org.eu
Email: secretariat@ecs-org.eu