ECS
EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## JANUARY EDITION: CHIEF INFORMATION SECURITY OFFICER (CISO)

Chief Information Security Officer (CISO)

# 2023 CONTENT

ECSO EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
01 101
Digital Forensics Investigator
01010 11101 00101
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. CISOs often struggle to find peers from other European countries. Consequently, ECSO launched "ECSO's CISO Community" in April 2022. This is the only European cross-sector and cross-country CISO Community that is hosted by a non-profit organisation and privileged partner of the European Commission in developing the European Cybersecurity Ecosystem. ECSO's CISO Community currently hosts 250+ CISOs (or equivalent) from 27 European countries. The Community serves as a place for cybersecurity leaders to exchange information, good practices, threat intelligence and to develop common positions of the practitioners in cybersecurity. Daily discussions are provided on topics of general interest to CISOs with a variety of backgrounds, experience levels and countries. ECSO helps in conveying a unified voice of practitioners towards other stakeholders in cybersecurity. Read more about ECSO's CISO Community, HERE, HERE and HERE.
2. In October 2022, ECSO organised its first CISO meet-up event with 96+ participants coming from various EU countries. This represented the kick-start for high-level discussions and trust-building. Throughout 2023, ECSO will organise several smaller sector-specific events for CISOs, with the CISO Meetup remaining the annual flagship event. For more information about ECSO's CISO Meetup 2022, see HERE.
3. In 2021, ECSO launched a survey targeting 100+ CISOs covering a wide range of topics. The survey encouraged CISOs to provide feedback on different aspects of their day-to-day work and encountered challenges. The survey also demonstrated the wide support for the establishment of a European CISO Community. See the full survey HERE.
4. Additionally, in early 2022, ECSO conducted a series of interviews. According to CISOs the most pressing area is cloud security and the biggest challenge faced in their industry is IT-OT integration. Areas that CISOs consider as most important in EU’s cybersecurity legislation are "harmonised legislation" and "minimum security standards". CISOs consider proactive engagement in a community of professionals as essential for improving threat information sharing across sectors and countries.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# What cyber threats will affect SMEs in 2023?

CYBER SECURITY
AGENCY OF
CATALONIA

The Cybersecurity Agency of Catalonia, through the company campaign #Negocibersegur, is publishing an article on the CIC4Cyber Data Science and Analytics service forecasting for 2023.

The document contains up-to-date information and prognosis on the most relevant factors in computer security that a CISO-as-a-service must take into account to support an SME.

The Cybersecurity Agency of Catalonia considers that knowing cyber security prospects is essential so that organisations can prepare to counter potential incidents.

More information HERE.

Chief Information
Security Officer (CISO)

# CISO could be a service?

Enterprise companies are under pressure to both avoid cyber incidents and comply with regulations and directives. However, limited budgets often force them to prioritise investments, making the role of the Chief Information Security Officer (CISO) increasingly important. However, not all companies can afford to have a dedicated CISO. Small and medium-sized businesses may struggle to afford the cost of a full-time CISO, as well as the implementation of other security controls. To address this, there are "CISO-as-a-Service" options available to help companies manage IT security at 360 degrees across the organisation, coordinate all stakeholders, and optimise investments.

The starting point for that initiative is the Exprivia Cybersecurity Framework, that helps organisation to understand the threat exposure and the level of maturity against known best practices and standards and helps to identify and prioritise initiatives in the Cybersecurity field.

More information HERE.

# Global Cyber Alliance: The Cybersecurity Career Path

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. Global Cyber Alliance is proud to be a founding partner alongside the World Economic Forum, Salesforce, and Fortinet. The Cybersecurity Role - Quick Look module provides information on relevant skills and associated roles for those just starting out.

Read more about it HERE.

# (ISC)$^2$ presents Common Body of Knowledge and CISO Leadership Certificates

(ISC)$^2$ CISSP Common Body of Knowledge (CBK) can be used by an aspiring CISO to identify the key skills and knowledge areas from ECSF CISO Profile, which can be found HERE. The CBK also serves as an excellent reference tool that documents peer-reviewed and widely-accepted industry standards and practices.

(ISC)$^2$ CISO Leadership Certificates help prepare future CISOs by providing knowledge and real-world application of cybersecurity management principles from an executive management point of view. This series bridges the gap between cybersecurity and business functions to help CISOs better understand and communicate best practices while maintaining focus on business operations. Certificates serve as a pathway to (ISC)$^2$ CISSP certification and demonstrate commitment to professional development.

Chief Information Security Officer (CISO)

# Resources from the Community

## Combatting digital fatigue in a time of increased cybersecurity complexity

The shift to remote and hybrid working, in conjunction with an increasingly digital world, has placed CISOs under greater pressure than ever. Cyber threats are growing increasingly complex, and the demand for cyber security skills is higher than ever. At the same time, digital fatigue is pushing cybersecurity professionals closer to burnout. So what is the answer? Learn more  HERE.

## The CISO's role in changing the board's perception

Having a CISO is crucial to any large entity's safe and secure running. Moreover, since the global pandemic struck, the breadth and depth of the CISO's job description have changed dramatically - they are no longer merely charged with heading up cybersecurity, they are now responsible for securing multiple devices, connections, and apps that are outside the organisation's perimeter. More about it HERE.

## Prodaft: Reports on current threats and APT's.

PRODAFT periodically publishes reports on current cyber threats and APTs that are relevant for both the public and law enforcement entities. As a threat intelligence company, we focus on providing intelligence-led insights that cut through the noise and help CISOs understand the organizational structures, attack vectors, motivations, infrastructures and operational details of the current threat groups. Recently revealing such information on the notorious threat actor FIN7, our report(s) can be found HERE.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## February Edition:
## Cyber Incident Responder

# 2023 CONTENT

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

1. The European Union Agency for Cybersecurity (ENISA) has a Computer Security Incident Response Teams (CSIRT) Maturity Framework. The Framework is intended to contribute to the enhancement of the global capacity to manage cyber incidents, with a focus on CSIRTs. The establishment of national CSIRTs is an essential step to facilitate the building of cyber capacity both within and across nations and make it more effective. The ENISA CSIRT Maturity Framework is aimed at parties involved in planning, building and leading such capacities with a concrete focus to increase maturity of all CSIRTs in the CSIRTs Network. Read it here.
2. The European Central Bank's (ECB) Banking Supervision has implemented a cyber-incident reporting framework. All significant institutions from the 19 euro area countries are required to report significant cyber incidents within two hours of classifying the incident as significant. This enables the ECB's supervisors to identify and monitor trends in cyber incidents affecting significant institutions and to gain a deeper knowledge of the cyber threat landscape. It also puts us in a position to be able to react more swiftly to a potential crisis caused by a cyber attack. Read more here.
3. In January 2022, the European Systemic Risk Board (ESRB) recommended establishing a pan-European systemic cyber incident coordination framework (EU-SCICF). The official recommendation can be read here. Major cyber incidents have the potential to corrupt information and destroy confidence in the financial system, and they may therefore pose a systemic risk. This calls for a high level of preparedness and coordination among financial authorities in order to respond effectively to such major cyber incidents. The EU-SCICF would aim to strengthen this coordination among financial authorities in the European Union, as well as with other authorities in the Union and key actors at international level. It would complement the existing EU cyber incident response frameworks by addressing the risks to financial stability stemming from cyber incidents. Read more here.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# “Cyber-Physical Detection and Response (CPDR) for Smart Manufacturers”

EXALENS®

Exalens has developed a cybersecurity solution for smart manufacturers facing threats to their connected physical operations. The platform autonomously detects and classifies the source of abnormal behaviour across IT, OT, and IoT cyber-physical processes. Its AI engine informs users whether a cyber attack, machine failure, system fault, or configuration error is affecting their operations and how to best respond.

This innovative technology learns any discrete process and can monitor more than 40 anomaly models. Its autonomous root cause analysis feature will spot threats and alert IT and OT teams in seconds, reducing incident response times by more than 80%. The alerts are comprehensive for every team and there is no added infrastructure required for implementing the solution.

Manufacturers can now maximise their production and build resilience by spotting the root cause of threats and responding faster.

Find out more here.

Cyber Incident Responder

# The importance of Cyber Incident Responder

exprivia

Impossible to avoid an attack but a proper incident detection and response can minimise the impact of an incident. We also need to keep in consideration that incidents are often correlated and therefore responding to an incident includes all the activities to analyse the incident and identify all possible correlations of the incident with other incident inside or outside the enterprise. In this contest it is relevant not just the technologies to identify IoC and correlate events, flow, incidents but also cooperation between different institutional and private CSIRT. Increasing the efficiency in the response requires as much as possible automation either at all level, from SOAR to XDR

Exprivia has a CSIRT portal which offers reporting, scanning and support services.

I am interested to learn more here and here.

Cyber Incident Responder

# The Cybersecurity learning Hub

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 Security Operations Engineer Trailmix to find out what it's like to be an incident responder. 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.

Cyber Incident Responder

# Professional Development Courses Offered by (ISC)2 to Encourage Successful Cyber Incident Response

(ISC)2 has offerings available t0 help organisations identify an incident and design and implement a comprehensive cybersecurity incident response plan.

Responding to a Breach is an interactive, immersive course that takes participants inside a cybersecurity breach scenario and helps them to design their own cybersecurity incident response plan. Participants will apply a phased approach to various types of cyber incidents and experience how different roles within the organisation (CEO, CISO, COO, etc.) might be involved, prioritise and react during a cyber incident.

All courses are free for (ISC)2 members and available for purchase for non-members. For additional information on professional development courses, visit the (ISC)2 Professional Development Institute.

(ISC)2 Incident Management: Preparation and Response Certificate is a self-paced immersive training course that helps learners define a security incident, prevent an incident from becoming a breach and identify how to leverage an incident to improve an organisations' security posture.

Cyber Incident Responder

## WithSecure helps customers reduce the cost and impact of compromises by rapidly containing and eradicating their adversaries

WithSecure provides co-security services that businesses need to minimise the impact of a cybersecurity breach. Clients of our Incident Response and Readiness services are able to minimise business disruption, understand why the incident happened and improve their security posture. That’s why so many of our partnerships have lasted over a decade.

We often publicly talk and write about our incident response experiences, including the articles in our "True Forensics" series.

To support incident response teams, we also open-source our tools, such as Chainsaw, which is a command-line tool providing a fast method of running Sigma and other rule detection logic over Windows event log data to highlight suspicious entries, and CatScale, which stands for "Compromise Assessments at Scale" and uses native binaries to collect data from Linux based hosts to determine the extent of a breach and find out if a given host has been compromised.

Cyber Incident Responder

# Resources from the Community

## Binalyze AIR: world’s fastest and most comprehensive DFIR platform

Digital Forensics & Incident Response (DFIR) is evolving to become fast, remote, integrated, and scalable across even the most complex of IT networks. This is why we built Binalyze AIR, the world’s fastest and most comprehensive DFIR platform. With 280+ evidence collected, our platform helps you analyse, investigate, collaborate, and complete compromise assessment and incident response investigations quickly. AIR saves you time, reduces cyber security operational costs, and helps you prevent financial and reputational losses. See more here and here.

## Incident response is key to any cyber security strategy

INo organisation is safe from attacks, regardless of their size, industry, or budget they have to spend on cyber security solutions. Savvy businesses understand that when it comes to breaches, the common maxim today, is that it’s no longer a case of ‘if’, but ‘when’, and ‘how often’. And although no company can afford to not have an incident response programme in place, many do not know where to begin. Read further to hear how you can help your company respond to, and prevent cyber incidents. Read more here.

Cyber Incident Responder

# The first line of defence against security incidents

Sababa Security

ITo prevent and respond to cyberattacks, companies must have an Incident Response Plan that should not only be developed in advance, but also clearly communicated to all levels of the organisation. And for each plan in place there must be a team capable of executing it. This is where the Cyber Incident Responder comes in. Find out more here.

Cyber Incident Responder

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## MARCH EDITION: CYBER LEGAL, POLICY AND COMPLIANCE OFFICER

Cyber Legal, Policy and Compliance Officer

# 2023 CONTENT

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

1. ECSO has a EU Legal & Policy Task Force. This task force supports ECSO Members in navigating complex regulatory environments while engaging with EU Institutions for better cybersecurity policies in the Union. ECSO gathers information and drafts actionable briefings for ECSO Members to anticipate key developments in European cybersecurity legislation. ECSO analyses both horizontal and vertical European cybersecurity legislation and engages with EU policy makers to help them draft cybersecurity policies that work for the European consumers and industry. Read more on the task force HERE.
2. ECSO has consulted with its diverse Membership on the CRA and has come forward with a position paper. The paper may be found HERE. ECSO supports the work done over the years by the European Union to secure the European Digital Single Market with legislations and investments, and continues to advocate for more European strategic autonomy, digital sovereignty and cyber resilience.
3. In their European Cybersecurity Skills Framework, ENISA brings up Cyber Legal, Policy and Compliance officer on page 9. In their summary of the skill, ENISA presents the mission, deliverables and the main tasks of the skill, including the key skills and knowledge needed for such a position. Read ENISA's summary of the skill HERE.
4. Close to the heart of a Cyber Legal, Policy and Compliance Officer, are European Policies and Regulations on the topic. ECSO invited you to read about policy actions taken on an EU level within cybersecurity HERE. The page provides insight into the EU Cybersecurity Strategy, the newly published NIS2 Directive for a high common level of cybersecurity across Europe, the European Cybersecurity Act and the European Certification Framework.

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# The importance of Cyber Legal, Policy and Compliance Officer

The Cyber Legal, Policy and Compliance Officer is responsible for ensuring compliance with legal frameworks and policies related to cyber security and providing legal advice for an organization's cyber security governance processes. This requires understanding business strategy and considering legal, regulatory, and privacy impact assessment requirements. Adapting to evolving directives, standards, and regulations requires significant expertise and ongoing training. This can be particularly challenging for smaller organisations with limited budgets. These organisations may turn to a Cyber Legal, Policy and Compliance Officer service to provide solutions that meet their needs, allowing them to focus on their core business while leaving the responsibility of cyber security to experienced third parties. This service offers dedicated time and activities for those who cannot hire a full-time professional.

Read more HERE.

Cyber Legal, Policy and Compliance Officer

# Learn new skills and what it's like to be a Cybersecurity Compliance Analyst! (FOR FREE!)

GLOBAL CYBER ALLIANCE

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 Cybersecurity Compliance Analyst Trailmix to find out what it's like to work in legal, policy and compliance. 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.

Cyber Legal, Policy and Compliance Officer

# Proofpoint Offers a Smarter Way to Stay Compliant with New Intelligent Compliance Platform

Today's organisations are overwhelmed with growing volumes of data that are incredibly difficult to manage. For Compliance and Legal staff, that means having to manually search and review petabytes of messages or files from regulatory compliance, supervisory, or investigation review queues.

To address this challenge, Proofpoint recently launched its new Intelligent Compliance Platform, which offers enterprises modern regulatory compliance safeguards while simplifying corporate legal protection practices. The platform leverages Proofpoint's proprietary machine learning engine to provide business leaders with AI-powered collection, classification, detection, prevention, search, eDiscovery, supervision, and next generation predictive analytics while meeting complex compliance and information governance obligations.

This enables Compliance, IT, Information Management, and Legal teams to gain visibility and access information with superior fidelity and context to growing volumes of enterprise data while detecting and preventing corporate and regulatory risks in real time.

Read more about it HERE.

# Resources from the Community

## The Cyber Law Expert: The Importance of a Cyber Legal, Policy, and Compliance Officer in Today’s Business Environment

In today’s digital age, where businesses and individuals rely heavily on technology, cybersecurity has become a critical concern: the threats are on the rise, and organisations need to ensure that they have the right measures in place to protect their digital assets. This is where Cyber Legal, Policy, and Compliance Officers come in. Find out more HERE.

## Compliance with privacy and compliance laws is key in today’s digital age

A skyrocketing number of data breaches have seen organisations in every sector race to address an array of compliance requirements, resulting from acts such as the European Union’s General Data Protection Regulation (GDPR) and others. This has given rise to several new roles within businesses, such as Head of Compliance or Chief Privacy Officers, who are tasked with maintaining legal compliance with data privacy laws and ensuring breach prevention. More about it HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## APRIL EDITION: CYBER THREAT INTELLIGENCE SPECIALIST

# 2023 CONTENT

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
01 101
01010 11101 00101
Penetration Tester

# Did you know?

1. ECSO is leading the effort to organise a pioneer **alliance of EU companies to share CTI at EU level**. ECSO Members, in particular large suppliers, innovative CTI start-ups and the ECSO's CISO Community, expressed interest in creation of an initiative to share CTI at EU level to improve the cyber resilience of the EU society and economy. Read more about the new initiative HERE and HERE.
2. There is currently a large **fragmentation, with different CTI approaches across Europe** on the private sector side, European private players, while often having individual capabilities, do not have a common cooperative platform for collaboration, losing opportunity for maximising effects of their actions.
3. ECSO received a lot of interest for CTI collaboration coming from EU and national public institutions. That can unlock potential for mutually beneficial process of sharing intelligence and collaborating with the public sector.
4. There are three overarching, but not categorical - classes of cyber threat intelligence (CTI)
   - **Tactical**: technical intelligence (including Indicators of Compromise such as IP addresses, file names, or hashes) which can be used to assist in the identification of threat actors.
   - **Operational**: details of the motivation or capabilities of threat actors, including their tools, techniques, and procedures.
   - **Strategic**: intelligence about the overarching risks associated with cyber threats which can be used to drive high-level organisational strategy.

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Global leader: managed detection and response capability

accenture

In Accenture, our cyber threat intelligence specialists proactively hunt for cyber threats, analyse and deliver actionable intelligence services and products – providing decision advantage to mitigate threats, enhance security posture, and reduce business risk. Finding cyber talent has been a difficulty for many organisations and Accenture is optimising the knowledge of our threat intel specialists and latest technology.

An example of that which we would like to highlight, is our Managed detection and response capability. Accenture has been identified as a global leader by Everest group report.

- Everest Group PEAK Matrix® for Managed Detection and Response
- Cyber Resilience Capabilities

Cyber Threat
Intelligence Specialist

# Threat Modelling for Telco

ERICSSON

We have previously written about the need for a telco-specific Threat Modelling framework – an important aspect of Threat Intelligence. Today there are two industry initiatives addressing this challenge: MITRE FiGHT™ (5G Hierarchy of Threats) and GSMA MOTIF (MObile Threat Information Framework).

MITRE FiGHT™: MITRE published FiGHT at the end 2022. Since there are no publicly reported attacks against 5G, FiGHT is based on theoretical research; on threats from legacy networks; and on operational assumptions such as compromised network functions.

GSMA MOTIF: The GSMA Fraud and Security Group has created a working group that is building a framework based on MITRE ATT&CK. The starting point is to focus on attacks observed in the wild for all mobile generations in order to have a realistic threat modelling.

Both MITRE FiGHT and GSMA MOTIF are beneficial, despite starting from different perspectives. Ideally, they should converge. MITRE is participating in GSMA MOTIF.

Cyber Threat Intelligence Specialist

# Cyber Threat Intelligence Specialist

exprivia

Cyber Threat Intelligence Specialists use their expert knowledge of malicious software to research and analyse cyber threats, reporting their findings to the team, using this intelligence to predict similar attacks, and ultimately helping to combat cybercriminal activities for their organisation.

Exprivia has created an API-based Threat Intelligence and Malware Analysis service: the Exprivia Threat Intelligence API. Thanks to the two implemented APIs, the system will be able to automatically analyse IPs, domains, Hash or files to understand whether they are affected by malware and implement defensive measures to neutralise it.

In synergy with Exprivia's CyberSecurity Observatory, the data collected from this activity is normalised and reported in the "Threat Intelligence Report," a report containing attacks, incidents and privacy violations in the Italian, Spanish and Brasilian territories.

More HERE.

Cyber Threat Intelligence Specialist

# Learn new skills and what it’s like to be a Cyber Threat Intelligence Specialist! (FOR FREE!)

GLOBAL
CYBER
ALLIANCE™

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 find out what it’s like to work in 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.

Cyber Threat
Intelligence Specialist

# Professional Development Courses Offered by (ISC)2 to Leverage Cyber Threat Intelligence

(ISC)2 has offerings available for cybersecurity professionals looking to understand more on how to leverage the Intelligence Cycle to communicate key elements of a cyber event.

Leveraging the Intelligence Cycle - This course is designed for cybersecurity professionals with knowledge of cyber concepts. Participants compare the various intelligence disciplines and learn to leverage the Intelligence Cycle to outline the when, why and how of cyber events. Free for (ISC)$^2$ members. Available to non-members for $80.

Utilising Big Data - For a limited time, non-members get free access to this course which provides an overview of Big Data components, architectures and applications. Learn to apply the concept of data flows to help defend organisations successfully managing and analysing large amounts of data. Designed for cybersecurity engineers and architects.

Cyber Threat
Intelligence Specialist

# Resources from the Community

## SMARTEX2 – Vulnerability Intelligence Reinvented

hackuity

Hackuity's Smart Exposure Explorer (SmartEx2) enables your teams to evaluate the real threats posed to your attack surface by each of the known 200,000 CVEs:

+ **Real exploitability**, clearly indicating whether a CVE is exploitable by attackers.
+ **Exploit maturity**, based on the number of exploits available to APTs or ransomware gangs.
+ **Threat intensity**, via information drawn from public social networks, the dark web, and the deep web.

Discover more HERE.

## Every business needs cyber threat intelligence specialists

itrainsec

The rapidly-evolving nature of cybersecurity has forced organisations of all sizes and in every industry to adapt and enhance their defences to stop confidential data from being exfiltrated and vulnerabilities from being exploited by attackers. Information security practitioners use the threat intelligence that is gathered by cyber threat intelligence specialists to gain critical insights that help them protect their organisations against the scourge of cybercrime. Learn more

Discover more HERE.

## Threat Intelligence Without Blind Spots – Insights Right from the Source

PRODAFT's main product, a cyber threat intelligence platform U.S.T.A., can efficiently address different challenges of security, risk, and fraud professionals - due to a meticulous composition of four main modules with different technological infrastructures. U.S.T.A. gives companies the ability to protect themselves against cyber threats and other APTs well in advance. Monitoring all corners of the deep and dark web, U.S.T.A. can alert customers about any suspicious activity that is precisely user-relevant, not merely general.  More information about the platform in their BROCHURE.

## The Essential Role of a Cyber Threat Intelligence Specialist for Effective Cybersecurity

In today's digital age, cybersecurity has become a top concern for organisations of all sises and industries. The rise of cyber threats has created a need for professionals who specialise in the collection, analysis, and dissemination of intelligence related to cyber threats. This is the role of a Cyber Threat Intelligence Specialist. Read more HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## MAY EDITION: CYBERSECURITY ARCHITECT

Cybersecurity Architect

# 2023 CONTENT

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
01
101
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. The main purpose of a cybersecurity architect skill is to plan and design security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls. More HERE.
2. Other titles for cybersecurity architect are " cybersecurity designer" and "data security architect". More HERE.
3. ECSO currently has ongoing work on software supply chain security. A technical paper will be released soon. We believe that this paper will be beneficial for Cybersecurity Architects in their role, as well as in raising awareness on the skill itself. We invite you to keep an eye out on ECSO's publication page HERE and social media channels HERE and HERE for its release.
4. ECSO has a technical workgroup "SRIA and cybersecurity technologies" with projects where a cybersecurity architect's skills are needed. The working group is divided into the following sub-groups: Ecosystem, Digital Transformation in Verticals, Data & Economy, Basic & Disruptive Technologies, and Cybersecurity for Dual Use Technologies. More on this technical working group may be found HERE. We invite you to contact roberto.cascella(at)ecs-org.eu for more information or with questions on how to get invlolved.

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Cybersecurity architect and risk management

Security is all about risk management. Unfortunately, organisations tend to relate security only to the internet and the cyberworld. However, it’s not just cybersecurity! Hence, it’s critical for an enterprise to understand that security is not solely about data, applications and infrastructure. It is also about securing customers, protecting organisational reputation, instilling trust and so on. How to solve that then? An enterprise security architecture can provide transparency in the alignment of measures in the security layer, such as security alerts, towards high-level business targets, like maintaining consumer trust. And when it comes to security architects, they are the key in breaching that gap and ensuring that security is imbedded in the optimal way.

Read more HERE and HERE.

# Cybersecurity Architect can help an organisation

A cybersecurity architect is responsible for designing, building, and maintaining the security systems within an organisation's IT network, including computer systems and data security. They design, lead implementation, and maintain security solutions that follow best practices and security controls, including security strategies for identity, device, data, application, network, infrastructure. They also design solutions for governance and risk compliance (GRC), security operation center, and security posture management.

Our cybersecurity architects can help an organisation in conduct cyber risk assessment, design and implement security controls, provide cybersecurity awareness, develop and implement a comprehensive cybersecurity strategy, develop incident response plans. Learn more HERE.

# Learn new skills and what it's like to be a Cybersecurity Architect! (FOR FREE!)

GLOBAL CYBER ALLIANCE

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 Cybersecurity Architect Trailmix to explore how to create enterprise information security architecture that aligns to business strategy and information security. 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.

Cybersecurity Architect

# CheckerSat, a cybersecurity solution for critical infrastructures

gmv®
INNOVATING SOLUTIONS

Antimalware solutions are often installed in critical infrastructures. However if someone attacks a critical infrastructure they would never use a malware which can be detected by COTS available technology. Instead, a targeted attack would be custom developed to avoid detection. Additionally, they need to be regularly updated with new signatures. This task requires special procedures to move the signatures from the Internet into the isolated critical infrastructure network. CheckerSat is a whitelisting solution designed to efficiently protect critical infrastructures against advanced threats. They change the protection paradigm from a known bad to a known good. Unlike antiviruses, only approved operations (i.e. known good) are allowed and all the rest is discarded. CheckerSat controls processes running in the systems, incoming and outgoing connections, integrity of system files, disk encryption and use of USB devices protecting the asset from a wide range of threats in a single agent. Discover more HERE.

# Professional Development Courses Offered by designed for chief security architect or analysts.

(ISC)2 has courses available for cybersecurity architects or analysts looking to advance their knowledge on a variety of topics including technologies, regulations, standards and practices.

CISSP-ISSAP Training Course Outline - For cyber professionals who hold the CISSP designation, Participants will be able to create an Information Security Architecture meeting the requirements of governance, compliance and risk management, develop an infrastructure security program, integrate security principles into applications development and more. This course is an online, self-paced course.

Certified Cloud Security Professional (CCSP) - This certification is ideal cybersecurity professionals responsible for applying best practices to cloud security architecture, design, and more. It is offered in three ways. Self-paced, online instructor-led, or classroom based. The CCSP demonstrates advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures.

# Resources from the Community

## Blue Team - SOC

The INSSIDE Cybersecurity Defence Center actively and multi-platform monitors to prevent, detect, analyse, and alert threats to strengthen and sustain a resilient ecosystem. The INSSIDE Cybersecurity Architect is responsible for designing and overseeing security infrastructure, identifying and mitigating vulnerabilities, implementing solutions, and monitoring network and system security. They seek to strengthen their commitment to their clients' security and stay at the forefront of cybersecurity trends. Read more HERE.

## Designing a Secure Future: The Role of Cybersecurity Architects in Innovation

Ensuring efficient technology implementation and usage across the organisation, Cybersecurity Architect is a crucial role, especially when companies transform or adapt. Indeed, they are responsible for designing and implementing secure computer systems, networks, and software applications that align with the organisation's business objectives and security requirements. More HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## JUNE EDITION: CYBERSECURITY AUDITOR

Cybersecurity Auditor

# 2023 CONTENT

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. The Main role of a Cybersecurity Auditor is to perform cybersecurity audits on the organisation’s ecosystem. This entails conduct of independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. An Auditor evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations. More HERE.
2. ECSO's Working Group 1 "Standardisation, Certification and supply Chain Management" is of interest to Cybersecurity Auditor's seen as it is a community of certifiers, test labs, component manufacturers, system integrators, service providers, national public administrations, RTOs, etc. that contributes to activities for pre-standardisation and supports the development and use of trusted European certified solutions across the supply chain and the various sectors. This Working Group supports the roll-out of EU ICT security certification schemes, standard and legislative recommendations, and ensures the establishment of trusted and resilient supply chains in Europe. More on this Working Group HERE.
3. Another activity of interest for Cybersecurity Auditors is ECSO's new Position Paper on the Cyber Resilience Act (CRA). ECSOs new publication can be found HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# What does a Cybersecurity Auditor do?

Cybersecurity auditor work with companies and organisations to provide audits of online security systems that typically include: a detailed report on existing cybersecurity systems, analysis of the efficient and effective operation of systems, recommendations on changes to protocols and infrastructure.

They must be able to analyse complex information, identify risks, provide solutions to mitigate those risks, communicate effectively with stakeholders at all levels of the organisation.

Our Cybersecurity auditors are updated with the latest security threats through our Threat Intelligence Report that we disseminate quarterly, giving them the ability to stay informed of trends and technologies in order to provide effective security controls.

Certifications provide objective validation of knowledge and skills as a cybersecurity.
Exprivia has certified employees and these demonstrate our expertise in the field and provide organisations with confidence in your ability to conduct effective security audits.

We invite you to read more HERE.

Cybersecurity
Auditor

# Learn new skills and what it’s like to be a Cybersecurity Auditor! (FOR FREE!)

GLOBAL
CYBER
ALLIANCE™

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 Cybersecurity Compliance Analyst Trailmix to learn about the role of the cybersecurity auditor - evaluating IT systems and applications against applicable cybersecurity rules and regulations. You can learn more about compliance and regulation with this module and you can 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.

More about Global Cyber Alliance HERE.

Cybersecurity
Auditor

# Professional Development and Cybersecurity Certifications for those with a cybersecurity auditor specialty.

CISSP: The Official (ISC)2 CISSP training provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam. This training session is ideal for those currently working as a security auditor or looking to pursue a career as a security auditor among many other positions.

CSSLP: Recognizes expertise and ability to incorporate security practices — authentication, authorization and auditing — into each phase of the software development lifecycle.

A Security Professional’s Guide to AI: This course introduces the details of data science in AI, its frameworks and languages and the challenges that security professionals face when working with AI development teams. Security professionals with an interest in AI including IT audit, development and operations should take this course.

# Cybersecurity auditor: Taking away the complexity

The role of a cybersecurity auditor is a loaded one, akin to how a city planner from the distant past would look at the intrusion protection of the city. Of course testing for the protection of a city would be laborious. But protecting a collection of software components and systems is easier.

What if the natural separation of concerns, that is, breaking down a complex audit process into manageable, low-cost intrusion simulations, makes auditing the myriad of components and services that incorporate IT, straight forward?

Since in software, unlike any other domain, we can simulate any intrusion path and test repeatedly. This substantiates that we can test our risk analysis of different security breaches and perform tests that are commensurate with the reward of the intrusion.

Ulysses Systems is a Maritime software specialist currently pioneering fast development of new annexes to existing software, including monitoring underlying systems for cybersecurity compliance.

Read more about it HERE.

Cybersecurity Auditor

# Resources from the Community

## Governance, Risk and Compliance

INSSIDE

The area defines cybersecurity strategies, consulting and regulatory alignment to security frameworks. Being certifiers of PCI SSC standards, clients are accompanied in the audit, advisory and support processes to properly manage governance and regulatory compliance. In addition, there are specialists in the analysis and identification of regulations and risks applicable to each business, the implementation of measures to mitigate them and the supervision and monitoring of regulatory compliance. More information HERE.

## Businesses: Neglect cybersecurity audits at your peril

itrainsec

For businesses that rely on data-driven operations, undergoing cybersecurity audits is non-negotiable. These audits play a critical role in addressing security issues and ensuring compliance with laws and regulations. By thoroughly examining various aspects of the company's IT infrastructure, audits aim to safeguard data assets and enhance defences against data breaches and other potential threats. However, in an ever-evolving threat landscape, with increasingly complex environments, audits are not without their challenges. Learn more HERE.

# Safeguarding Digital Assets in a Complex Landscape with the Cybersecurity Auditor

Sababa Security

With cybersecurity threats being more and more pervasive across IT, OT, and IoT domains, organisations are increasingly prioritising robust cybersecurity measures. In this context, the role of a cybersecurity auditor has become indispensable, being essential for assessing a company's security posture, identifying vulnerabilities, and ensuring compliance with cybersecurity regulations and industry best practices. Learn more HERE.

Cybersecurity Auditor

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## JULY EDITION: CYBERSECURITY EDUCATOR

Cybersecurity Educator

# 2023 CONTENT

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

1. A Cybersecurity Educator designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. He/she use effective teaching methods to enhance the cybersecurity culture, capabilities, and skills of personnel, while promoting its importance and integration within the organisation. Alternative titles are " Cybersecurity Awareness Specialist", "Cybersecurity Trainer", and "Faculty in Cybersecurity (Professor, Lecturer)". More HERE.
2. ECSO has a "Skills & Human Factors" Working Group that is beneficial for Cybersecurity Educators. Its aim is to enhance cybersecurity capacity for a resilient digital Europe through education, training, skills development, and inclusivity. To get involved in this working group, ECSO invites you to contact its Head of Sector Nina Olesen at **nina.olesen@ecs-org.eu**.
3. ECSO has multiple initiatives aiming to raise awareness and educate. ECSO's Youth4Cyber initiative educates and raises the awareness of young people (6 to 26-year olds) on cybersecurity. The European cybersecurity community is invited to contribute to this catalogue and showcase their work. Additionally, ECSO is involved in the project SuperCyberKids that provides children ages 8 to 13 and their teachers with an educational ecosystem of cybersecurity learning content.
4. ECSO has also launched the European HR Community that is free to join. This Community regularly organises webinars to raise awareness on the challenges faced by HR and to propose solutions (eg. Demystify the CISO role: CISOs and HR managers combining forces). In Autumn 2023, the Community will organise training and awareness sessions for HR practitioners to empower them with best practices, insights and valuable lessons to improve hiring and retention of cyber talents. Stay tuned! To join this community, send an e-mail to Arnaud de Vibraye at **arnaud.de.vibraye@ecs-org.eu**.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Keeping employees aware of individual and collective responsibilities

accenture

Every enterprise today operates in a world filled with potentially harmful intrusions, malware and other security risks. That’s why at Accenture, our more than half million employees are a key line of defense against cyberattacks. Our global workforce has a critical mission to understand current and emerging cyber threats and take ongoing action to ensure enterprise safety. We must keep all employees aware of their individual and collective responsibilities to keep information safe — an awareness that translates into organisational best practices. By blending cybersecurity awareness communications with exercises based on actual business situations, the custom-designed learning activities increase employee awareness of specific risks and promote stronger information about security practices.

Accenture also ensures locally that the knowledge is shared by being a member of several cyber organisations and communities, such as Cyber Security Coalition, sponsoring of the Belgian Cyber Security Challenge, collaboration with coding schools such as BeCode, etc.

- Strengthening our first line of cyber defense
- Cyber Security Coalition
- BeCode

# The Cybersecurity Educator

The cybersecurity educator is the figure within organisations charged with promoting and consolidating the importance of cybersecurity in terms of cybersecurity awareness.

The detailed objective is to design, develop and conduct awareness, training and education programmes on cybersecurity and data protection.

Exprivia in its Cybersecurity team has various Cybersecurity Educator resources with appropriate and certified skills who carry out Cybersecurity Awareness activities in private organisations, training organisations and public administration.

According to Exprivia's Cybersecurity Observatory, the most commonly used attack technique is phishing/social engineering. This confirms that the weakest link in the chain is the human factor and it is important to invest in this.

Exprivia provides its expertise through a Cybersecurity Academy, Cybersecurity Awareness activities. Read more HERE.

# Learn new skills and what it’s like to be a Cybersecurity Educator! (FOR FREE!)

GLOBAL CYBER ALLIANCE

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 Security Awareness Specialist Trailmix to learn about the role of the cybersecurity educator and what's involved in building a security-first culture within an organisation. 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.

Cybersecurity Educator

# Resources from the Community

## Cyber Resource Hub

Browse our curated guides, case studies, webinars, reports, and other resources – all designed to help bring clarity to your cyber vulnerability chaos. From ASM to VM to MITRE ATT&CK, get insights from 17x Microsoft MVPs and best-in-class cybersec teams, and walk away with actionable strategies for your own organisation. Discover Hackuity's Cyber Resource Hub HERE.

## Awareness Campaign

We define and execute plans and awareness actions that allow the organisation's human resources to become the first line of defence against cyber threats. We work comprehensively with automated platforms, webinars and talks. We run phishing and ransomware attack simulation campaigns, aligning ourselves with our clients' HR and Internal Communications departments. Read more HERE.

## The crucial role of cybersecurity educators in safeguarding today’s digital world

itrainsec

In today’s highly connected world, where technology plays is infused into every aspect of our lives, the significance of cybersecurity is underestimated at our peril. And with the escalating frequency and complexity of cyber threats, the need for skilled experts in this field has skyrocketed. However, too often the importance of cybersecurity educators goes unrecognised. These dedicated individuals are the unsung champions who play a pivotal role in preparing and cultivating the future generation of cybersecurity professionals, empowering them to protect the digital frontiers of our world. More HERE.

## Nurturing a Cybersecurity-Conscious Workforce: The Key Role of a Cybersecurity Educator

Sababa Security

As the human factor still drives many cyber incidents, developing a cybersecurity-conscious culture within a company becomes of paramount importance. And that’s where the Cybersecurity Educator comes in. This role plays a crucial part in raising awareness about the importance of cybersecurity among employees, helping them understand the risks and consequences of potential threats, become proactive in identifying and reporting them, and take appropriate actions to protect the organisation’s assets. More HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## AUGUST EDITION: CYBERSECURITY IMPLEMENTER

Cybersecurity Implementer

# 2023 CONTENT

ECS
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

1. A Cybersecurity Implementer provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. They ensure adherence to specifications and conformance requirements, along with sound performance. They also resolve technical issues required in the organisation's cybersecurity-related solutions. More HERE.
2. Some alternative job titles to Cybersecurity implementer are: Information Security Implementer, Cybersecurity Solutions Expert, Cybersecurity Developer, Cybersecurity Engineer, and Development, Security & Operations (DevSecOps) Engineer.
3. ECSO's Working Group 1 "Standardisation, Certification and supply Chain Management" is of interest to Cybersecurity Implementors seen as it is a community of certifiers, test labs, component manufacturers, system integrators, service providers, national public administrations, RTOs, etc. that contributes to activities for pre-standardisation and supports the development and use of trusted European certified solutions across the supply chain and the various sectors. This Working Group supports the roll-out of EU ICT security certification schemes, standard and legislative recommendations, and ensures the establishment of trusted and resilient supply chains in Europe. More on this Working Group HERE.
4. Additionally, ECSO's newest publication on Digital Twins (DTS) can be of interest to Cybersecurity Implementers. The publication analyses and discusses four different use cases covering the applications of DTS, intended as cyber-physical synergy, across a broad variety of sectors, inter alia: business, education and skills, collaborative industries, industrial cybersecurity. Read it HERE.

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

## Seamless DevSecOps: Empowering Secure, Automated, and Cloud-Driven Development Excellence

Development, Security and Operations (DevSecOps) converges application development, security, infrastructure as code, and operations into a continuous, end-to-end, highly automated delivery cycle. Embedding security into the product development life cycle helps protect the business while maintaining speed and assisting to eliminate friction.

– Defining the outcome and vision of DevSecOps in a measurable and objective way.

– Building technical enablers, capitalising on the transformation stage of Accenture’s cloud journey while “living in the cloud”.

– Driving adoption of the technical enablers.

- Moving the Enterprise to DevSecOps | Accenture
- Leveraging the power of technology for resilience
- Cloud Security Case Study: Zero Trust Strategy | Accenture
- IT Touchless Operations | Accenture
- US CSO50 2022 awards showcase world-class security strategies |

# What is OWASP Top 10, and do you need it to secure your application?

aikido

In the rapidly shifting digital landscape, application security is a necessity. One of the most effective ways to bolster your application's security is by evaluating it with the OWASP Top 10. But what exactly is the OWASP Top 10, and why should it matter to you?

The Open Web Application Security Project (OWASP) is a non-profit foundation that strives to make software on the web more secure. Their Top 10 is a widely recognised report that outlines the 10 most critical web application security risks. It's essentially a checklist of the most common weaknesses that could make your application a target for cyber threats.

Read more about it HERE.

Cybersecurity Implementer

# Cyber Diia implement a project for the requalification of Veterans

Diia Cyber

Russia's full-scale invasion of Ukraine has led to a dramatic increase in the number of war veterans struggling to reintegrate into civilian life.

In response to these urgent concerns, a robust partnership has been forged among Cyber Diia, the Ministries of Digital Transformation and Veterans, in conjunction with the non-governmental organisation Scientific Association for Cybersecurity and Chemonics International.

As part of this initiative, a comprehensive three-month retraining program has been devised for veterans, which will operate across six centers situated in esteemed Ukrainian universities. The program's primary objective is to equip veterans with the skills necessary to work as proficient system administrators in both the public and private sectors. Furthermore, participants will receive essential psychological and legal support to facilitate their transition. Additional programmes will focus on critical infrastructure  security and resilience. This initiative aims to provide new opportunities for veterans as they transition to civilian life."

Find  more information HERE.

Cybersecurity Implementer

# Resources from the Community

# Blue Team

The cybersecurity implementer administers, manages and optimises cybersecurity platforms and processes. In turn, defines, provides and implements solutions. Discover more HERE.

## Navigating the Evolving Ransomware Landscape: The Critical Role of Cybersecurity Implementers.

Cybersecurity Implementers are frontline defenders against rising ransomware threats. Their vital role shields businesses from evolving risks, especially with the surge of double extortion tactics. Data exposure and encryption amplify dangers, bolstered by ransomware-as-a-service. Amidst these escalating challenges, cybersecurity implementers must proactively safeguard systems and data to counter persistent peril. Learn more HERE.

Cybersecurity Implementer

# Enhancing Cybersecurity: The Crucial Role of Cybersecurity Implementers in Comprehensive Protection

Sababa
Security

Technology alone is not enough to ensure robust cybersecurity. The proper configuration, monitoring, and continuous management of security systems are essential components of a comprehensive cybersecurity strategy. This is precisely where the Cybersecurity Implementer comes in. Find out more HERE.

Cybersecurity
Implementer

ECS
EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## SEPTEMBER EDITION: CYBERSECURITY RESEARCHER

Cybersecurity Researcher

# 2023 CONTENT

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
01 101
Digital Forensics Investigator
01010 11101 00101
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

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# 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)

# A new standard for lightweight authorisation and access control

ERICSSON

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.

Cybersecurity
Researcher

## Cybersecurity Researcher

exprivia

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.

Cybersecurity
Researcher

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

GLOBAL CYBER ALLIANCE™

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.

Cybersecurity
Researcher

# ISC2 Professional Development Opportunities and Cybersecurity Certifications for Cybersecurity Researchers

(ISC)$^2$

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.

Cybersecurity Researcher

# 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 empoderate 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

Cybersecurity Researcher

# 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 - Security & Protection for All

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 vulnerabilites in systems and investigating malware. They also analyse 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.

## Automatic Runtime security for containerised workloads

Quritis

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

HWG Sababa

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.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## October Edition: Cybersecurity Risk Manager

# 2023 CONTENT

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. A Cybersecurity Risk Manager handles the organisation's cybersecurity-related risks aligned to the organisation's strategy. They also develop, maintain and communicate the risk management processes and reports. More HERE.
2. Some alternative job titles for "Cybersecurity Risk Manager" are: Information Security Risk Analyst, Cybersecurity Risk Assurance Consultant, Cybersecurity Risk Assessor, Cybersecurity Impact Analyst, and Cyber Risk Manager. More HERE.
3. Depending on the interest of the Cybersecurity Risk Manager ECSO has two Working Groups where they may contribute within their field to European cybersecurity as a whole. The first Working Group is dedicated to research and new technologies. 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 Risk Managers 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 on this Working Group HERE
4. The second ECSO Working Group of interest for a Cybersecurity Risk Manager is dedicated to cyber resilience of economy, infrastructures and services. In its vision to have a trusted environment for practitioners and end-users in cybersecurity to share information, lessons learned and best practices to increase cyber resilience of European companies and organisations, it is essential to receive input from Cybersecurity Risk Managers. In this working Group, they may engage with ECSO's CISO Community, the SOC/CTI Task Force, and experts within the NIS2 Directive. More HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Cybersecurity Risk Manager

accenture

Today's risks are complex and interconnected, with new risks emerging rapidly. Volatility is increasing, along with regulatory pressure. We have seen major disruptions to business cycles over the last three decades, including the dot-com crash, the global financial crisis and the recent Covid-19 pandemic. Volatility seems likely to increase, along with threats from known and unknown places. Regulation is unlikely to become less complex or less demanding. In this environment, every organisation needs to improve its risk management capabilities.

We work with Chief Finance Officers, Chief Risk Officers and other senior risk and compliance executives to help them manage their risk agenda across five key areas: Cyber Risk, Operational Risk & Resilience, Fraud & Financial Crime, Regulatory & Compliance and Financial Risk.

|!| Interesting finding: Cyber transformers are six times more likely than the rest to apply leading risk management practices (65% vs. 11%) read more here and on our State of Cybersecurity Resilience 2023 report.

- Compliance Risk Study - 2022 | Accenture
- Call for change: Managing ICT governance and risk – UNIQA Case Study
- The Cyber-Resilient CEO (accenture.com)

Cybersecurity Risk Manager

# Cybersecurity Risk Manager energy domain

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

In today's digital world, managing cyber risks has become increasingly crucial, and the energy sector is particularly vulnerable to cyber-attacks. These attacks can have severe consequences for both energy supply and public safety. Operators managing critical infrastructures in the energy sector must remain vigilant and protect against cyber threats. To help EPES (Electrical Power and Energy Systems) operators with this task, the CyberSEAS research project develops a risk assessment tool. The tool follows the guidelines set by the ISO31000 standard and includes several steps. It identifies assets using MITRE ATT&CK mapping, it assesses asset vulnerabilities using the Common Vulnerability Scoring System and a Cyber Maturity Model questionnaire. It also calculates probability and financial impacts, identifies risk profiles to prioritise, and identifies countermeasures based on cost-benefit analysis. This tool can help energy operators understand the potential risks and impacts of cyber-attacks and provide a systematic approach to managing and mitigating them.

I am interested in learning more HERE.

Cybersecurity Risk Manager

# Learn new skills and what it’s like to be a Cybersecurity Risk Manager! (FOR FREE!)

GLOBAL CYBER ALLIANCE™

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 Cybersecurity Risk Manager Trailmix to learn how and what it’s like to manage risks associated with digital business assets. You can also check out other cybersecurity roles and learn vital skills for free whilst you’re there!

Cybersecurity Risk Manager

# ISC2 Professional Development Opportunities and Cybersecurity Certifications for Cybersecurity Risk Management

CGRC Certification - The CGRC certification is a proven way to demonstrate your knowledge and skills to integrate governance, performance management, risk management and regulatory compliance within your organisation. Learn how to utilise frameworks to integrate security and privacy within organisational objectives, better enabling stakeholders to make informed decisions regarding data security, compliance, supply chain risk management and more.

Risk Manager Practioner Certificates - The ISC2 risk management certificates provide an understanding of how to assess and analyse risk, and take a deeper dive into standards and risk methods to ensure cybersecurity practitioners are ready for success. There are three risk manager practioner certificates available.

Governance Risk and Compliance Skill Builders - ISC2 offers 11 skill builders on cybersecurity risk management that are created by industry experts and available now on demand. Earn CPE Credits with these short-format learning courses.

# Resources from the Community

## The Role of a Cybersecurity Risk Manager in the Modern Digital Landscape

HWG Sababa

In today's hyper-connected world, where technology fuels every aspect of our lives, the need for robust cybersecurity measures has never been more critical. Businesses, governments, and individuals are increasingly reliant on digital infrastructures, making them susceptible to a myriad of cyber threats. In this context, the role of a cybersecurity risk manager emerges as a keystone, ensuring the security and resilience of organisations against evolving threats. More HERE.

## Governance, Risk & Management

INSSIDE

We define cybersecurity strategies, consulting and regulatory alignment to security frameworks. Also, we implement methodologies and execute services of analysis and risks management, DRP, BCP, BIA/RIA. We rely on our Insside Security Suite platform (ISS), Risk Management Module. Learn more HERE.

## Empowering Cybersecurity Risk Managers: The Essence of Digital Forensics and Incident Response

Cybersecurity Risk Managers play a crucial role in ensuring organizational safety amidst digital chaos. One indispensable tool in their arsenal is Digital Forensics and Incident Response (DFIR). DFIR isn't just a theoretical concept; it involves diving hands-on, quite literally, into the digital realm. By gaining in-depth knowledge of DFIR, Cybersecurity Risk Managers transform into digital detectives, comprehending the nuances of cyberattacks and mastering the techniques to combat them. itrainsec offers online training that equips teams and individuals with this essential knowledge. More HERE.

## BLINDSPOT: Game-changing Risk Intelligence at Your Fingerprints

BLINDSPOT is a next-generation risk intelligence platform, created with the goal of providing users with a holistic assessment of any organisation’s cyber risk level. In the growing landscape of sophisticated supply chain attacks, we understood the need to oversee the interconnected systems between organiations and their suppliers, vendors, and third and fourth parties. The platform monitors contemporary incidents and predicts subsequent adversarial activities - therefore preventing software and physical supply-chain attacks and detrimental breaches worldwide. See more HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## NOVEMBER EDITION: DIGITAL FORENSICS INVESTIGATOR

Digital Forensics Investigator

# 2023 CONTENT

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. The main role of a Digital Forensics Investigator is to connect artefacts to natural persons, capture, recover, identify and preserve data, including manifestations, inputs, outputs and processes of digital systems under investigation. He/She also provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.  More HERE.
2. Some alternative titles to a Digital Forensics Investigator are: “Digital Forensics Analyst”, “Cybersecurity & Forensic Specialist”, and “Computer Forensics Consultant”. More HERE.
3. The European Anti-Fraud Office (OLAF) has digital evidence specialists that provide both its investigators and its external partners with practical support for digital forensics (identification, acquisition, imaging, collection, analysis and preservation of digital evidence). More on their procedures HERE.

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Digital Forensics Investigator

accenture

Combining, market-leading advanced analytics and intelligent automation with managed security services, Accenture´s cyber resilience incubation centers help organizations out-innovate attackers every single day!

The Cyber Fusion Centers (CFC) is where we highlight the best of Accenture Security. We do this by demonstrating the depth of our skills and experience through storytelling, interactive workshops, and demonstrations of our latest innovations and core hosted capabilities, including FusionX’s Cyber Incident Forensic Response (CIFR), FusionX’s Advanced Adversary Simulation, iDefence and our security futurists at Accenture Labs.

*See our industrialized, proven managed security services in action! Collaborate with our global security ecosystem and experience how persistent, 24/7 vigilance can give you the confidence you need to focus on your business, rather than the threats to it. You can do so in our Cyber Fusion Centers | Accenture in: Australia, Brazil, Czech Republic, India, Israel, Italy, Japan, Spain and in two locations in the USA.*

- State of Cybersecurity Resilience 2023
- Everest Group PEAK Matrix® for Managed Detection and Response
- Cyber Resilience Capabilities

01
101

Digital Forensics
Investigator

# Digital Forensics

Exprivia's incident response services cover the entire phase from discovery to incident management, forensic services, and advanced malware analysis to quickly understand the nature and origin of the attack:

- Incident response services identify a rapid and effective strategy, reducing the impact on business and supporting in the remediation and recovery phase of the systems;
- Threat intelligence services collect information on new and existing threats concerning the customer;
- Forensic analysis services include legal computer expertise, acquisition, duplication, and data extraction with repeatable techniques and methodologies, analysis of operating systems, analysis of unauthorised system access. Creation and protection of the integrity of the chain of custody of evidence sources and digital evidence.

Read more HERE.

GLOBAL
CYBER
ALLIANCE™

# Learn new skills and what it’s like to be an Cyber Defense Forensics 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 Get Started with Cyber Defence Forensics trail to learn how cyber defence forensics improves an organisation's cybersecurity and what’s needed to prepare for a career as a cyber defence forensics analyst. You can also check out other cybersecurity roles and learn vital skills for free whilst you’re there!

# ISC2 Professional Development Opportunities and Cybersecurity Certifications for Digital Forensics Investigators

Forensics Data Acquisition – This Express Learning course explains the digital forensics scientific process, data acquisition methods, and digital evidence handling and preservation principles. It is critical that security professionals understand the technical, legal, and administrative challenges facing data forensics to protect the information gathered prior to it being turned over for analysis to ensure the evidence holds up in a court of law. This course is ideal for cybersecurity professionals with a beginning level of knowledge of digital forensic concepts.

SSCP ISC2 Certification - The SSCP is the ideal certification for security professionals with proven technical skills and practical, hands-on security knowledge in operational IT roles. It confirms a practitioner's ability to implement, monitor, and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. Intended for professionals who have a minimum of one-year cumulative work experience in one or more of the seven domains of the SSCP CBK.

Digital Forensics
Investigator

# Resources from the Community

## Exploring the Role of Digital Forensics Investigators

HWG Sababa

The rise of cybercrime poses significant threats to individuals, organisations, and nations. Amidst the digital battleground, Digital Forensics Investigators employ their expertise to expose the truth hidden within the digital realm. Ensuring that cybercriminal investigations reveal all digital evidence necessary to demonstrate malicious activities, these experts bridge the gap between digital artefacts and individuals, capturing, recovering, identifying, and preserving data related to digital systems under examination. See more HERE.

INSSIDE

## Red Team

Our Digital Forensics Investigator are responsible for collecting, analysing, and preserving digital evidence from computer systems and networks to investigate or prevent criminal or fraudulent activities. They preserve evidence from emails, documents, or chats, and then analyse it for legal cases or incidents involving other hackers. Read more HERE.

01
101

Digital Forensics
Investigator

# Digital Forensics Pros Bolster Ransomware Defence with Key Skills

itrainsec

Digital Forensics Investigators must grasp Ransomware prevention fundamentals to proactively safeguard digital systems. Acquiring knowledge in cybersecurity measures, encryption protocols, and user awareness enables investigators to anticipate and counteract potential threats. By understanding the nuances of Ransomware prevention, these professionals can effectively analyse and respond to cyber incidents, mitigating risks and ensuring the integrity of digital environments they investigate. Keeping this in mind, itrainsec has a ready-made online training course 'RANSOMWARE: GUÍA DE SUPERVIVENCIA' (Ransomware: Survival Guide). Learn more HERE.

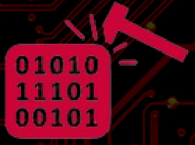
01
101

Digital Forensics
Investigator

ECS
EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY AWARENESS CALENDAR 2023

## December Edition: Penetration Tester



Penetration Tester

# 2023 CONTENT

ECS
EUROPEAN CYBER SECURITY ORGANISATION

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

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester

# Did you know?

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. A Penetration Tester plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).. More HERE.
2. Some alternative job titles for “Penetration Tester” are: “Pentester”, “Ethical Hacker”, “Vulnerability Analyst”, “Cybersecurity Tester”, and “Red Teamer”. More HERE.
3. ECSO has a Working Group, named Trusted Supply Chains, that is dedicated to building a stronger and more resilient cyber-Europe where trust is established all along the supply chain by reflecting market needs, best practices and challenges. Penetration Testers can participate in this working group and provide valuable insights on methodologies & recommendations to support the development of a trusted supply chain and manage the risks of products and services. This will be achieved by analysing the technical impact of EU legislations and policy initiatives and by fostering cooperation with SDOs, European institutions and agencies. More on this Working Group HERE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

# Resources from our Members

# Advanced Protection with Specialised Penetration Testing Services

Penetration testers play a crucial role in defending IT infrastructures against potential threats, helping organizations improve their security posture.

At Exprivia, we offer various Penetration Testing services:

1. Web Application Penetration Test: We identify vulnerabilities in web applications by exploiting incorrect configurations or outdated software, etc.
2. Exploit Use on Windows, Linux, and Mac OS X: We leverage known vulnerabilities to access systems and retrieve sensitive data without authorization.
3. Network Traffic Penetration Test: We intercept unencrypted network traffic to recover sensitive data, using network sniffing tools and Man In The Middle attack techniques.
4. Password Penetration Test: We enhance password security using fast crackers to perform Brute Force attacks and identify weak passwords.
5. Malvertisement: We create and send fake emails with links to identify users who click on suspicious links without checking the sender.

Discover more HERE.

Penetration Tester

# Learn new skills and what it’s like to be a Penetration Tester! (FOR FREE!)

GLOBAL CYBER ALLIANCE

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 Penetration Tester Trailmix to learn what it’s like to be a penetration tester - finding vulnerabilities and determining weaknesses to improve an organization's defences against cyber attack. Learn what’s involved and what’s needed to prepare for a career as a penetration tester. You can also check out other cybersecurity roles and learn vital skills for free whilst you’re there!

Penetration Tester

# ISC2 Professional Development Opportunities and Cybersecurity Certifications for Penetration Testing

ISC2 offers Web Application Penetration Testing. This is a self-paced Express Learning online training professional development course. The course will acquaint participants with web application penetration testing and introduce a hands-on perspective of how a penetration tester applies methodology with practice to test web applications for security flaws. This course is free for ISC2 members.

Earn .5 CPE credits with ISC2 Skill Builders
Software Security: Fixing Forward at Scale in Real Life
This course demonstrates that investing in software security can build trust with users, ensure compliance with industry standards and help security professionals stay ahead of potential threats. Combining testing, tools and human ingenuity can safeguard against threats.

The Future of API Security
Learn how implementing cybersecurity best practices including penetration testing, secure coding and monitoring for suspicious activity and audits to secure APIs can protect against threats and vulnerabilities.

# Resources from the Community

## Securing the Digital Frontier: Penetration Testers' Crucial Contributions Unveiled

HWG Sababa

Penetration testers play a crucial role in assessing the effectiveness of security controls, revealing vulnerabilities, and evaluating the criticality of these vulnerabilities if exploited by threat actors. With the digitalization of industrial facilities, development of smart cities, and widespread adoption of IoT devices, the scope of their skill application expands. Find out more here. More HERE.

## Red Team - Pentesting

INSSIDE

We work on infrastructure, systems and web applications with the aim of finding vulnerabilities that could be exploited by an attacker. We also evaluate the exposed surface and analyze the assets that could be attacked. Furthermore, we evaluate and guide the mitigation and remediation actions of the detected vulnerabilities. Learn more HERE.

01010
11101
00101

Penetration Tester

# Web Developers' Cybersecurity Boost: Key for Effective Penetration Testing

itrainsec

A strong foundation in cybersecurity for web developers enhances the skill set of penetration testers, enabling them to approach security testing with a deeper understanding of the systems they are assessing. This interdisciplinary knowledge is valuable for creating more effective security strategies and fostering collaboration between security and development teams. Keeping this in mind, itrainsec advises penetration testers to get training in CYBERSECURITY FOR WEB DEVELOPERS. More HERE.

01010
11101
00101

Penetration
Tester

# 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

company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu