EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Research topics

ENISA Threat Landscape

Overview

New concepts and ideas are evolving in the cybersecurity domain due to research and innovation activities conducted by academics, industry and professionals around the world. These are important steps since the pace of innovation from adversaries (e.g. malicious actors) is higher than the one from cybersecurity specialists finding solutions to deter them. In fact, apart from basic cybersecurity hygiene and training, investing in research and innovation is the most viable option for defenders to come closer to what is required to improve the security of cyberspace. In this report, we highlight some of the most important cybersecurity research and innovation topics explored in the EU and around the world.

Better understanding of the human dimension

Cybersecurity is still seen as the practice of protecting networks, information systems and data (NIS). This definition needs to be further expanded beyond technical issues to include socio, behavioural and economic concerns and the different roles performed by the parties involved. This should constitute a priority in future cybersecurity research and innovation discussions. A better understanding of the human dimension is key in the definition of any cybersecurity strategy so that security decisions are taken to meet their needs, skills and expectations.

Cybersecurity research and innovation

During 2019, we observed an increase in the number of test labs and cyber-ranges[1] becoming available on-premises and in cloud offerings. These are essential resources for researchers to simulate attacks, develop exploitation scenarios, obtain operational data and test defence strategies in a multipurpose virtual environment. However, existing testing environments lack on replicating many vulnerabilities that typically compromise security such as human and engineering factors, among others. To improve efficiency, it is import to research and innovate the scope and fidelity of these test labs and propose new technical solutions.

Overview

5G security

The rollout of 5G mobile networks in some countries started in 2019 but the expectation is for the number of installations to increase in 2021. This next generation of mobile communications is of paramount importance for the social and economic progress of the European Union. Hence, the future research and development of 5G security solutions is crucial for the sustainability and reliability of this technology. In 2019, ENISA published a threat landscape for 5G networks reviewing some critical security aspects related with this emerging technology.[2] Key topics in research and innovation of 5G security should consider the following aspects.

- The research and development of security controls to cover the protection of the network, physical elements and data layers, thus providing a multi-layer protection solution. With 5G Networks, data will be located in centralized cloud servers, intermediate fog nodes, and edge devices, increasing complexity in the implementation of a security solution.
- The research and development of standards and requirements for security controls to implement across interconnected networks with multiple owners, topologies, operators, and a diversified variety of devices and network layers.
- The research and development of key management capabilities enabling secure interoperability between nodes connecting resource-limited edge and IoT devices. This capability should include effective access control, authentication, cryptography, and key management techniques to limited-resource nodes.

EU research and innovation projects on cybersecurity

- The EU is working to establish a pilot for a cybersecurity competence network. CONCORDIA[3], ECHO[4], SPARTA[5] and CyberSec4Europe[6] are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call for 'establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap'. The EU expects to strengthen its cybersecurity capacity and address future cybersecurity challenges with these four pilot projects, for a safer EU Digital Single Market.
- The EU grants €38 million for protection of critical infrastructure against cyber threats. The European Commission has announced that it is committing more than €38 million through Horizon 2020 to the EU's research and innovation programme. The program is meant to support several innovative projects in the field of protection of critical infrastructure against cyber and physical threats and making cities smarter and safer.[7]
- The EU launched a €10.5 million call for projects in cybersecurity. The Commission has launched a new call worth €10,5 million through the Connecting Europe Facility (CEF) programme for projects that will work on stepping up Europe's cybersecurity capabilities and cooperation across member states.[8]

CTI research and innovation

Rapid dissemination of CTI methods and content

Various research needs were identified during the reporting period and the actions to address these needs are proposed here. These have been grouped into some categories to better reflect the scope better. Though not overlap-free, these categories are indicative for areas of potential CTI improvements.

- **The results of research projects in the area of CTI need to be assessed and mapped to a broader CTI context** to identify overlaps and gaps and to make them comparable with existing CTI commercial products, services and practices. This will help to disseminate the results to the user community. At the same time, existing gaps will be filled by additional functions, content and processes. EU (Horizon H2020) projects with CTI relevance are excellent candidates for this task, contributing to improving CTI practices.
- **The provision and use of open-source CTI material should be promoted**. This will facilitate knowledge transfer, but it will also lower the threshold of CTI skills. Open-CTI is the perfect candidate for this purpose, as it supports the ingestion of CTI from multiple sources into a single base that can be shared among various users, while at the same time offering a set of functions for managing this information. By adopting Open-CTI, users will be in a position to obtain valuable information at a relatively low skill threshold.

_Research resulting in emerging trends

The need to **strengthen CTI** with other established cybersecurity tools requires the structural and contextual evolution of this domain. At the same time, technological advances brought by emerging technologies pose the question of how CTI can benefit from these developments. Thus, **prospective research** needs in the area of CTI will contribute to improving processes, functions, automation, content structure and validation, service delivery, speed-to-user/dissemination, CTI deployment and mappings.

CTI has been firmly established in the cybersecurity domain as an essential tool for enhancing agility and efficiency in defending cyberattacks.

CTI research and innovation

Functionality, level of automation and compliance with maturity requirements

- **Process automation will assume a key role in CTI**. While modern cyberattacks have become heavily automated, organisations try to defend themselves against them manually or by partially using automation. This is an unequal contest, which slows down the speed and capability of responding. Investigating the potential automation of CTI processes will be vital for striking a balance between attackers and defenders. Achieving this will need a thorough analysis of CTI process steps and options for automating these steps via available and emerging technologies.
- **CTI maturity requirements will need to be identified in further detail**. Although some criteria/requirements for the selection of CTI functions (e.g. Threat Intelligence Platforms or TIPs) have been developed for various CTI user profiles, similar requirements will be necessary for further CTI products, services and tools. Such requirements will be associated with multiple levels of user maturity and expenditure and types of CTI. Similar criteria/requirements are necessary for various other elements of a CTI infrastructure, such as tools, good practices, sharing platforms, etc. Hence, apart from the development of CTI capability maturity models, research is needed to show how CTI functions correspond to the various CTI maturity levels. This work will contribute to increasing the speed of adoption of CTI practices.
- **The use of AI/ML in CTI should be further investigated**. This will reduce the number of manual steps in CTI analysis and will increase the value of ML functions within CTI activities.

Building bridges to related areas

- **Novel approaches for the ingestion of CTI knowledge by domains** that can profit from it need to be developed. Examples are cyber-ranges, hybrid threats, supply chains and geopolitical assessments and crises. Questions to be asked in this respect include: What are the points at which CTI can be taken into account? Which CTI content is relevant? What are the validation criteria for the appropriateness of CTI information? How can CTI be 'hooked' into information about the domain concerned? What kind of information from those domains can be added to CTI? The synergies reflected in these questions may boost use-cases and content quality in an omnidirectional manner.
- **CTI is essential for a number of disciplines**. Examples include risk assessment/management and the definition of protection requirements and certification. It will be beneficial for those disciplines to use CTI in the correct way. CTI contribution to these disciplines can be identified using information, such as threat models, threat actor information (capabilities, motives), attack methods and exploits. Although some relevant material does exist (e.g. ATT&CK attack framework[9]), significant work is required in order to identify and standardise such information interfaces.

CTI research and innovation

Effectiveness of CTI operations

- **Methods for using CTI effectively will be a tool for decision-making**. Such methods of deploying CTI efficiently will help decision-makers to understand the value of CTI and practitioners to evaluate the return-on investing in CTI. Such methods/KPIs will need to consider factors beyond the CTI content, taking into account improvements achieved within the entire life cycle of security management and risk mitigation. Optimally, measuring the effectiveness of investment in CTI will be part of a much wider consideration of the economics of cybersecurity in various kinds of organisations (e.g. according to security requirements, maturity levels, etc.).

- Although low-cost tools prevail for aggregating, analysing and disseminating CTI, **some research may be necessary to find automated tools for managing the CTI** consumed and produced. Other than standardised data formats (e.g. CSV files, STIX, TAXII), standard CTI functions may be the subject of such research, followed by the development of low-cost, open-source tools supporting such functions.

Evolution of CTI structure and content

- As CTI is penetrating additional domains, **information from these contexts needs to be fed back to the original CTI knowledge base**. For example, CTI structures need to be defined to capture geopolitical and hybrid-threat information. The same applies to the relevance of CTI for risks, incidents, forensic analyses, assurance levels, etc. The existing CTI formats need to evolve to capture information emanating from these dependencies in CTI.
- **Emerging technologies such as AI** may be used to validate of analysed CTI. Such tools may augment or even replace manual CTI analysis, but also provide support throughout the life cycle of CTI (e.g. check the relevance of CTI based on existing incident information). Such novel approaches to CTI will enhance the quality and relevance of the information.

References

1. The Cyber Range concept was initially defined in 2013 by the European Defence Agency (EDA) in the report "Common staff target for military cooperation on cyber ranges in the European Union" as a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination.

2. "ENISA threat landscape for 5G Networks". November 21, 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4. https://echonetwork.eu/

5. https://www.sparta.eu/news/

6. https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

“CTI has been firmly established in the cybersecurity domain as an essential tool for enhancing agility and efficiency in defending cyberattacks.”

in ETL 2020

Related

READ THE REPORT

ENISA Threat Landscape Report
The year in review

A summary of the main cybersecurity trends for the year.

READ THE REPORT

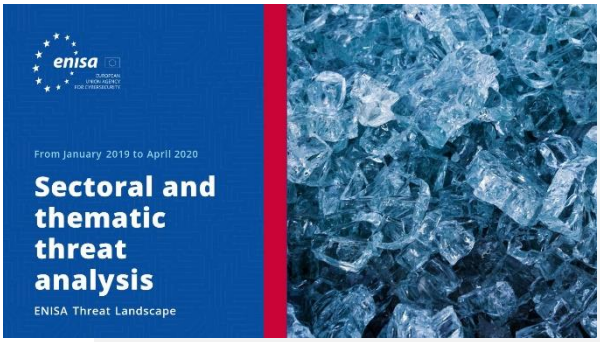
ENISA Threat Landscape Report
List of Top 15 Threats

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Main incidents in the EU and worldwide

Main cybersecurity incidents happening between January 2019 and April 2020.



READ THE REPORT

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

Other publications

Roadmap on the Cooperation Between CSIRTS and LE

A roadmap on the cooperation across CSIRTs in particular with national and governmental - law enforcement (LE) and the Judiciary.

READ THE REPORT

EU MS Incident Response Development Status Report

A study aiming at the analyses of the current operational Incident Response set-up within NISD sectors and identify the recent changes.

READ THE REPORT

ENSIA CSIRT maturity assessment model

An updated version of the "Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity" published by ENISA in 2017

READ THE REPORT

“The sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing and multi-stage attacks.”

in ETL 2020

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu