EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Cyber Threat Intelligence Overview

ENISA Threat Landscape

Overview

_Developments in the area of CTI

In this report, we **assess the state-of-play of cyber threat intelligence (CTI) as a dynamic cybersecurity domain**. This analysis aims to indicate the main trends in the expeditious development of CTI by providing relevant references and summarizing the next steps required to advance this topic during the coming years.

In January 2020, ENISA organized its **CTI-EU** community-bonding event. At this event, various presentations demonstrated the current state of play of CTI at commercial, institutional and user levels. Presentations, discussions and CTI vendor demonstrations addressed the status of products, approaches and practices and indicate existing issues. It is evident that **CTI has achieved a sufficient maturity and critical mass** of CTI-related material is now available, e.g. through current practices, tools and processes.

It seems that the **next challenge in CTI will be to digest, consolidate and disseminate existing practices** to achieve more extensive use in a cost-efficient and synergetic manner. The main opportunities in this respect lie in sharing non-competitive CTI practices, requirements, tools and information. Apart from this, identifying new stakeholders entering the CTI business - both producers and consumers – will enhance capabilities, identify standard CTI requirements and establish CTI sharing capabilities in a timely manner. Through both its CTI-EU event and cooperation with various EU stakeholders, ENISA plans to strengthen synergies and disseminate CTI good practices.

_CTI tools, material and practices

Commission Horizon 2020 research and framework_
Various CTI-related H2020 projects have been completed or are still in progress. They have already consumed significant funds and delivered a variety of tools and practices for producing, consuming and using CTI.

Practices of standardisation bodies, international, organisations, governments, industry, academia and individual users_ A variety of good practices have been developed covering: CTI methods, frameworks and process models[1,2,3] maturity issues, requirements, surveys of use, evaluation of tools[8,9,10], approaches to developing CTI[11,12] ,etc.

Open-source CTI offerings_ Various open-source feeds[13] and tools supporting OpenCTI[14], are important for producers and consumers, allowing for free access to valuable CTI at low cost.

Open-source CTI tools (and practices)_ Numerous open-source tools, practices and articles have been published[15,16], that provide practical approaches to CTI analysis and dissemination by using open-source tools.[17,18,19]

Overview

_CTI training opportunities

CYBRARY_ Introduction to Cyber Threat Intelligence.[21]

INSIKT_ Learning more about the “Cyber Threat Intelligence Certification Protocols”.[22]

SANS_ FOR578: Cyber Threat Intelligence.[23]

FIRST.org_ Cyber Threat Intelligence Symposium.[24]

Gov.uk_Cyber_ Threat Intelligence Training (CRTIA).[25]

ENISA-FORTH_ NIS (Network and Information Security) Summer School – Cyber Threat Intelligence Training.[26]

ENISA-FORTH Summer School 2019↗

CTI-EU Community Event 2020↗

_Gaps in available CTI material and practices

Despite the higher maturity levels achieved in CTI practices and tools and the provision and consumption of CTI, there are still gaps in CTI, in particular regarding various use-cases, sectoral CTI, and CTI types (operational, tactical, strategic), among others. Such a significant gap has been identified in discussion within ENISA CTI forum concerning the availability of **up-to-date CTI from attacks** on critical sectors and critical services. It has been agreed that CTI elements (e.g. tools, techniques and procedures or TTPs) included in various international good practices and frameworks (e.g. ATT&CK[28]) need to evolve to include intelligence from a wider spectrum of attacks. Particularly pressing are the CTI elements of various sectors and service-provisioning infrastructures and offerings. An example of this is the lack of emphasis on **attacks on cloud-computing**.[29] Similar requests may emerge from infrastructures that are either emerging (e.g. 5G[30]), or are of specialized nature yet play an essential role in critical industrial systems for example industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems).[31]

Although existing frameworks may contain various elements used in TTPs targeting such systems, their applicability in various sectors will need to be expanded to take account of the peculiarities of TTPs, such as the abuse of available application programming interfaces (APIs) and exploitation of core assets. Apart from TTPs, elements that will require further consideration are guidance on **prevention, detection and mitigation practices** for these sectors.

This will facilitate the development of the necessary capabilities and enable the use of CTI specifically crafted for these sectors. The main barrier to the dissemination of actionable CTI for various platform types and infrastructures is the lapse time between an incident, producing related CTI and populating this information to open-source tools. **Tighter coordination and cooperation** among the parties involved will reduce the time before CTI is made available to the wider user community. Building trust among participating entities is key to the accelerating the CTI supply chain. Identifying relevant players and mobilising the CTI community are important to facilitate these interactions.

Another barrier to building the necessary capabilities is the availability and consumption of CTI within various cybersecurity management activities. Examples include cybersecurity crisis management, incident management, incident response, threat hunting and vulnerability management. This deficiency was assessed in the previous ENISA Threat Landscape (ETL) report[32] by means of asynchronous cycles among cybersecurity disciplines and continues to persist.

Concluding this section, one should note that the deficiencies described are not due to a lack of CTI knowledge per se but rather to the lengthy cross- and intra-sector communication and coordination cycles for exchanging CTI knowledge.

Overview

_Issues emerging from building a CTI infrastructure

CTI is offered in some broad categories according to users' requirements for CTI, namely as operational, tactical and strategic. Existing commercial offerings consisting of tools for collection, maintenance, analysis and dissemination of CTI, CTI feeds, threat intelligence platforms (TIPs), etc., support some of these CTI types. However, there is no one-size-fits-all approach.

Existing offerings concentrate on operational and tactical CTI, while strategic CTI is mostly offered independently.

However, the boundaries between CTI are rather blurred. This has the effect that, when a CTI consumer wishes to build up a capability and the corresponding environment to manage CTI, selecting suitable elements is not straightforward. This is mainly because **CTI service provisioning and the existing CTI-tool landscape is somewhat fragmented**. In attempting to build up such an environment, CTI users will need to do so by selecting a 'best of breed' system from existing offerings. Their selection has to fulfil CTI requirements and the CTI practices and processes applied, while taking into the account their current and prospective CTI maturity objectives.

Although some criteria/requirements for selecting TIPs have been developed[33] for various CTI user profiles, similar requirements will be necessary for further CTI products, services and tools. Ideally, such requirements will focus on various levels of user maturity, levels of 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.

In the long run, OpenCTI[14] may be a good solution for addressing the issues caused by the fragmentation of CTI offerings, given its inherent capability to integrate CTI sources of various types into a single tooling environment.

In the coming year, ENISA and CTI stakeholders will put some effort into assessing the CTI infrastructure requirements and checking how they can be fulfilled by existing CTI products. This will begin with an attempt to establish a CTI infrastructure for ENISA's internal needs for developing a CTI platform for strategic CTI.

_Leveraging CTI in related cybersecurity disciplines

The incorporation of CTI into key cybersecurity disciplines has already been identified as an issue by members of the CTI community. This is particularly the case in security management activities and components that are related to highly dynamic environments with increased exposure, such as user devices (e.g. USIMS, security tokens, mobile devices, industrial systems, e-health devices, etc.). Other related disciplines that may significantly benefit from CTI are certification activities, crisis management practices, cyber-forensics and incident response, among others.

ENISA recognizes[35] the need for the **inclusion of CTI in the area of certification**. In 2020, ENISA established an ad-hoc working group aiming to integrate risk management and CTI with practices for identifying assurance levels.

In particular, the CSA states that ***'The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident'* (Art. 52(1)).**

This makes it evident that CTI needs to flow into the certification process using an assurance level evaluation. Although, parts of CTI are envisaged in certification standards[36] by using an 'attacker profile', this concept comprises a small part of available CTI.

The work performed by **ENISA's ad-hoc working group** consists of combining information from risk and threat assessments (CTI) to group protection requirements appropriately and map them on to various assurance levels. The mapping will be based on various risk levels that emerge from the threat exposure of assets and, at the same time, give rise to proposals for the number and strength of mitigation controls. These controls will drive the selection of security functions that will be assigned to multiple assurance levels and will be subject to implementation by the various targets of certification (ToCs).

ENISA's work on this topic is being undertaken with the support of an expert group, combining risk management, CTI and certification skills. The work started in April 2020 and will be completed in the third quarter of 2020. The results of this work will be published by ENISA.

Overview

_Results of a comprehensive CTI survey

From a representative CTI survey[7], numerous interesting conclusions on the current uptake of CTI practices and tools can be drawn. Among other things, the survey reflects the current state-of-play of CTI capabilities, the types of CTI used types of CTI used among stakeholders, the interplay of CTI practices with other processes in organisations and the use-cases of CTI tools.

In this discussion, the results of the survey are extrapolated to the experiences gained by ENISA within its own (strategic) CTI activities and the feedback from various CTI stakeholders within the EU and European CTI forums[36]. In this context, the focus is on identifying requirements, collecting information, producing strategic CTI, use of tools and practices and integration with other relevant processes. In this regard, we would like to highlight the following points.

- One of the main conclusion from this report is that **semi-automation of CTI production** is an important tool: while automation of information ingestion is increasing – despite an increase in CTI consumption by vendors – manual activities are still building the core of organisations' CTI production.

- Information aggregation, analysis and dissemination activities are managed using **widely available tools** such as spreadsheets, mail and open-source management platforms, which is indicative of the efficiency of low-cost solutions.

- The importance of defining **CTI requirements** is understood by the CTI user-community. This is in response to the repeated pleas of CTI experts[5,6] about recognising the significance of CTI requirements and shows that the CTI community has taken their advice. It is also interesting to see that a significant amount of CTI requirements reflects the needs of business and executives. This is an indication that CTI is becoming part of decision making at business and management levels.
- A combination of consumption and production of CTI is the prevailing method for building up an internal **CTI knowledge base**. An increase in organisations' own CTI production is the main trend, especially for CTI derived from their own analysis of raw data and contextualised threat alerts. Consumption from publicly available sources is becoming a trend, considering the growing use of available CTI (open-source CTI feeds as indicated in the point below).
- **Open-source information gathering** is the most widely used ingestion method, followed by threat feeds from CTI vendors. This is a clear upwards trend in 2020, indicating that CTI users are investing in their own capabilities to produce CTI that complies with their requirements.
- **Threat detection** is assessed as the main use case for CTI. Although indictors of compromise (IoCs) are still the most important elements of CTI in threat detection and threat response, threat behaviour and adversary tactics (TTPs), seem to be responsible for upwards trends in the use of CTI in organisations.
- Measuring the **effectiveness of CTI** is still a difficult task, and only a small percentage of CTI users (4%) implement processes to measure CTI efficiency. It is argued, that although tooling may add value in CTI analysis, the analyst's skills are most important for successful implementation of CTI. An interesting finding regarding the level of satisfaction is the low rating given to the value of machine learning functions.

_Conclusions and next steps

Having regard to all these developments in the area of CTI, the following conclusions can be drawn. From these conclusions, some next steps are indicated, at least from the point of view of ENISA, where CTI is going to be strengthened in accordance with its new mandate, but also taking into account the developments observed in its stakeholder communities, such as Member States, the European Commission and other European bodies, vendors and CTI end users:

- Given the increasing number of EU and Member States stakeholders, **cooperation and coordination of EU-wide CTI activities** is key. While building on synergies may reduce CTI costs, it also increases trust among CTI players, thus enabling the sharing of CTI and good practices. ENISA will promote cooperation with various stakeholders by initiating the **identification of CTI requirements.** This will include multiple stakeholders groups within the EU ecosystem of organisations (i.e. Commission, EU bodies, agencies and Member States).
- As the relevance of CTI for strategic and political decision-making is understood, it is important to **facilitate its connection with geopolitical information and cyber-physical systems**. This will enable the inclusion of CTI in decision-making processes, but it will also allow its context to be expanded to the identify hybrid threats.

- **Integrating CTI with security management processes** will help CTI to proliferate in related areas and will contribute to the timely identification, detection and prevention of threats. An immediate effect will be to increase the agility of rather long-lasting processes (e.g. certification, risk assessment). At the same time, CTI will facilitate emergency decision-making (e.g. crisis management) by providing evidence on exposure to cyber threats.
- To better respond to the increasing role of CTI, ENISA will be working on **building a comprehensive CTI programme**. The ENISA CTI programme will bundle internal skills horizontally to enrol all related stakeholders in all phases of CTI production and dissemination, and develop a CTI infrastructure that will be used for both internal and training purposes.
- Investment in some basic CTI concepts, in particular **CTI maturity and threat hierarchies**, is considered very useful for increasing the uptake of CTI. ENISA – together with its EU partners - will invest some effort into developing a CTI maturity model. Moreover, ENISA consolidate and disseminate useful multi-purpose CTI material such as threat hierarchies that can be used in other areas (e.g. certification, risk management, sectoral landscapes, etc.).

Some of the above conclusions and next steps will be the subject of ENISA's work in the area of CTI during the coming years.[35]

References

1. Cyber Threat Intelligence Lab" HPI and TU Delft. https://www.cyber-threat-intelligence.com/

2. "5-Step process to power your Cyber Defense with Cyber Threat Intelligence". March 12, 2020. EC-Coucil Blog. https://blog.eccouncil.org/5-step-process-to-power-your-cyber-defense-with-cyber-threat-intelligence/

3. "The Cycle of Cyber Threat Intelligence". September 3, 2019. SANS, https://www.youtube.com/watch?v=J7e74QLVxCk

4. "Maturing Cyber Threat Intelligence". HPI and TU Delft. https://www.cyber-threat-intelligence.com/maturity/

5. "Intelligence Requirements: the Sancho Panza of CTI". Andreas Sfakianakis. https://threatintel.eu/2019/09/24/intelligence-requirements-and-don-quixote/

6. "Your requirements are not my requirements". March 20, 2019. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. "2020 SANS Cyber Threat Intelligence (CTI) Survey". February 10, 2020. SANS. https://www.sans.org/reading-room/whitepapers/threats/paper/39395

8. "Most Important Cyber Threat Intelligence Tools List For Hackers and Security Professionals". September 9, 2019.Prodefense. https://www.prodefence.org/most-important-cyber-threat-intelligence-tools-list-for-hackers-and-security-professionals-4/

9. "What Is Threat Intelligence? Definition and Types". October 25, 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

10. "The Ultimate Guide to Cyber Threat Intelligence (CTI) in 2020" June 15, 2020.AI Multiple. https://research.aimultiple.com/cti/

11. "Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts". March 2019.NCSC. https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

12. "What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team". January 15, 2020. Recorded Future. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

13. "A List of the Best Open Source Threat Intelligence Feeds". March 4, 2020. Logz.io. https://logz.io/blog/open-source-threat-intelligence-feeds/

14. "Open Cyber Threat Intelligence Platform". OpenCTI. https://www.opencti.io/en/

15. "The Cyber Intelligence Analyst Cookbook Volume 1", 2020. The Open Source Research Society. https://github.com/open-source-rs/The-Cyber-Intelligence-Analyst-Cookbook/blob/master/The%20Cyber%20Intelligence%20Analyst%20Cookbook%20Volume%201%202020.pdf

16. "Open Source Intelligence (OSINT): A Practical example". March 16, 2020. Cyber Security Magazine. https://cybersecurity-magazine.com/open-source-intelligence-osint-a-practical-example/

17. "Cyber Trust". Cyber Trust. https://cyber-trust.eu/

18. “Why we’re part of CONCORDIA – Europe’s largest cybersecurity consortium”. December 11, 2019. Ericson. https://www.ericsson.com/en/blog/2019/12/concordia-telco-threat-intelligence-platform

19. “1st Newsletter of CYBER-TRUST project” Aditess. https://aditess.com/main/2020/01/30/1st-newsletter-of-cyber-trust-project/

20. CTIA Exam Blueprint v1. EC-Coucil. https://www.eccouncil.org/wp-content/uploads/2019/04/CTIA-Exam-Blueprint-v1.pdf

21. Intro to Cyber Threat Intelligence. Cybrary. https://www.cybrary.it/course/intro-cyber-threat-intelligence/

22. Learning More about The Cyber Threat Intelligence Certification Protocols. INSIKT. https://www.insiktintelligence.com/cyber-threat-intelligence-certification/

23. Cyber Threat Intelligence Summit. SANS. https://www.sans.org/event/cyber-threat-intelligence-summit-2020

24. FIRST Cyber Threat Intelligence Symposium. FIRST. https://www.first.org/events/symposium/zurich2020/program

25. Cyber Threat Intelligence Training (CRTIA). Gov.uk. https://www.digitalmarketplace.service.gov.uk/g-cloud/services/599285779458382

26. NIS Summer School – CTI Training. FORTH/ENISA. https://nis-summer-school.enisa.europa.eu/2019/index.html#program

28. MITRE. https://attack.mitre.org/

29. “The CTI Cloud context dilemma” January 2020. NetScope. https://www.enisa.europa.eu/events/2019-cti-eu/presentations/the-cti-cloud-context-dilema

30. “ENISA Threat Landscape for 5G Networks” October 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

31. “Applying Cyber Threat Intelligence to Industrial Control System”. September 19, 2019. CSIAC. https://www.csiac.org/journal-article/applying-cyber-threat-intelligence-to-industrial-control-systems/

32. “ENISA Threat Landscape Report 2018“ March 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

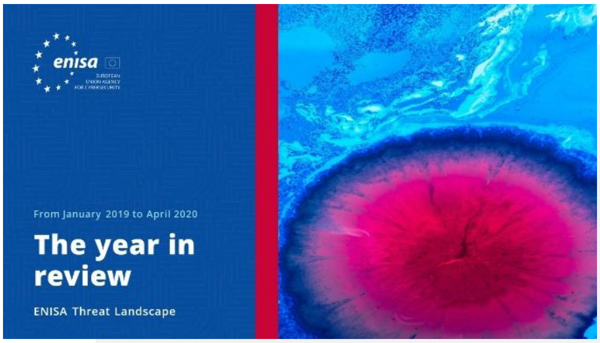
33. “Exploring the opportunities and limitations of current Threat Intelligence Platforms” March 26, 2018. ENISA. https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

34. “ENISA Programming Document” November 2019. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

35. “EU Cybersecurity Act” June 7, 2019. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

36. “CTI-EU | Bonding EU Cyberthreat Intelligence” https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence

Related



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

The year in review

ENISA Threat Landscape

ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

READ THE REPORT

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

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 EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

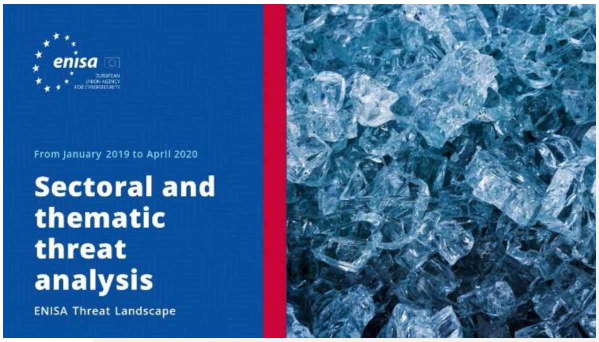
Research topics

ENISA Threat Landscape

ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and Cyber Threat intelligence.

READ THE REPORT



From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

READ THE REPORT

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

Contextualised threat analysis between January 2019 and April 2020.

From January 2019 to April 2020

Main incidents in the EU and worldwide

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Main incidents in the EU and worldwide**

Main cybersecurity incidents happening between January 2019 and April 2020.

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

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

Other publications

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ADVANCING SOFTWARE SECURITY IN THE EU

The role of the EU cybersecurity certification framework

NOVEMBER 2019

Advancing Software Security in the EU

Presents key elements of software security and provides a concise overview of the most relevant existing approaches and standards in the secure software development landscape.

READ THE REPORT

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

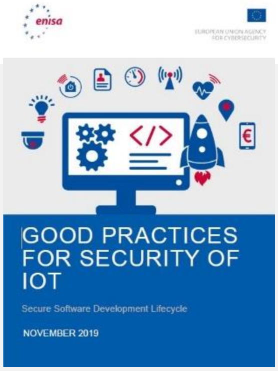
NOVEMBER 2019

ENISA good practices for security of Smart Cars

Good practices for security of smart cars, namely connected and (semi-) autonomous vehicles to enhance car users' experience and improve car safety

.

READ THE REPORT



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GOOD PRACTICES FOR SECURITY OF IOT

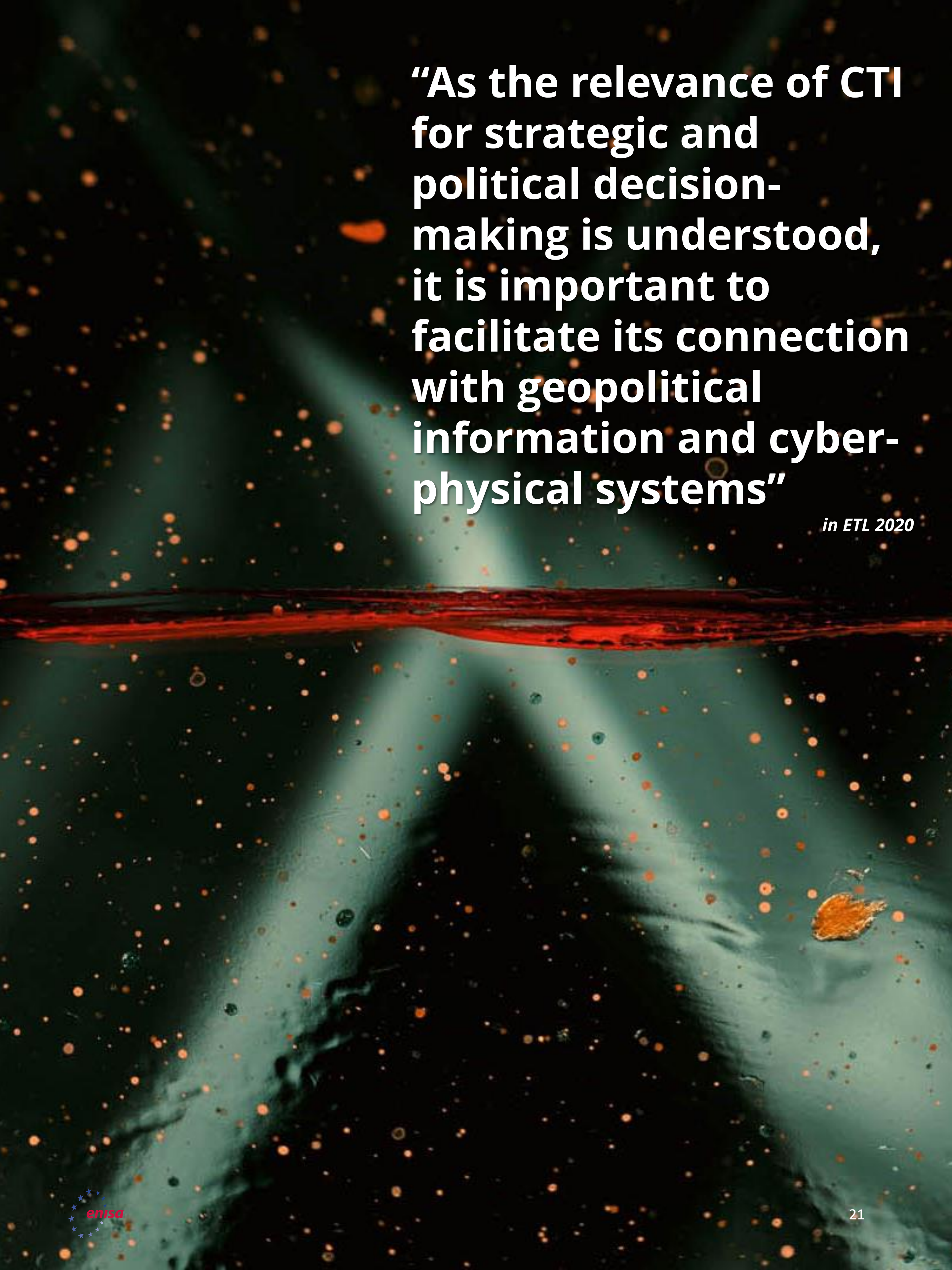
Secure Software Development Lifecycle

NOVEMBER 2019

Good Practices for Security of IoT - Secure Software Development Lifecycle

ioT security with a particular focus on software development guidelines.

READ THE REPORT



> “As the relevance of CTI for strategic and political decision-making is understood, it is important to facilitate its connection with geopolitical information and cyber-physical systems”
>
> ***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.

Copyright Notice

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