enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

Aperçu du renseignement sur la cybermenace

Paysage des menaces de l'ENISA

Aperçu

_Évolutions dans le domaine du CTI

Dans le présent rapport, nous **évaluerons l'état des lieux du renseignement sur la cybermenace (CTI - *Cyber Threat Intelligence*) comme domaine dynamique de la cybersécurité**. Cette évaluation vise à montrer les principales tendances dans le développement rapide du CTI en fournissant des références pertinentes et en résumant les prochaines étapes qu'il faudra mettre en œuvre afin de faire avancer ce dossier au cours des prochaines années.

En janvier 2020, l'ENISA a organisé son événement de cohésion communautaire: le **CTI-EU**. Lors de cet événement, diverses présentations ont été faites pour décrire l'état des lieux actuel du CTI au niveau commercial, au niveau institutionnel et au niveau des utilisateurs. Les présentations, discussions et démonstrations proposées par les fournisseurs de CTI portaient sur le statut des produits, des approches et des pratiques, tout en évoquant les problèmes existants. Il est évident que **le CTI a aujourd'hui atteint une maturité suffisante et qu'une masse critique** d'informations liées au renseignement sur la cybermenace est désormais disponible, notamment grâce aux pratiques, outils et processus actuels.

Il apparaît que le **prochain défi en matière de CTI consistera à assimiler, consolider et diffuser les pratiques existantes** pour permettre une utilisation plus large de manière rentable et synergique. À cet égard, les principales possibilités reposent sur le partage sans concurrence des pratiques, exigences, outils et informations concernant le renseignement sur la cybermenace. En outre, l'identification de nouvelles parties prenantes s'inscrivant dans l'activité du CTI (à la fois producteurs et consommateurs) permettra d'améliorer les capacités, d'identifier les exigences standard en matière de CTI et d'établir des possibilités de partage de CTI en temps utile. Grâce à son événement CTI-UE et à sa coopération avec diverses parties prenantes de l'UE, l'ENISA prévoit de renforcer les synergies et de diffuser les bonnes pratiques en matière de renseignement sur la cybermenace.

_Outils, matériel et pratiques en matière de CTI

Programme-cadre de recherche Horizon 2020 de la Commission_ Plusieurs projets H2020 liés au renseignement sur la cybermenace ont été réalisés ou sont toujours en cours de réalisation. Ceux-ci ont déjà mobilisé des fonds importants et fourni un grand nombre d'outils et de pratiques pour produire le CTI, le consommer et l'utiliser.

Pratiques des organismes de normalisation, des organisations internationales, des gouvernements, de l'industrie, des universités et des particuliers_ Diverses bonnes pratiques ont été développées sur les thèmes suivants: Méthodes, cadres et modèles de processus de CTI[1,2,3], questions de maturité, exigences, enquêtes d'utilisation, évaluation des outils[8,9,10], approches de développement du CTI[11,12], etc.

Offres CTI en open source_ Plusieurs outils et flux en open source[13] venant étayer OpenCTI[14] sont importants pour les producteurs et les consommateurs car ils leur permettent d'accéder librement et à faible coût à de précieuses informations sur la cybermenace.

Outils (et pratiques) CTI en open source_ De nombreux outils, pratiques et articles en open source ont été publiés[15,16], qui fournissent des approches pratiques d'analyse et de diffusion du CTI à l'aide d'outils en open source.[17, 18,19]

Aperçu

_Possibilités de formation au renseignement sur la cybermenace

CYBRARY_ Introduction au renseignement sur la cybermenace.[21]

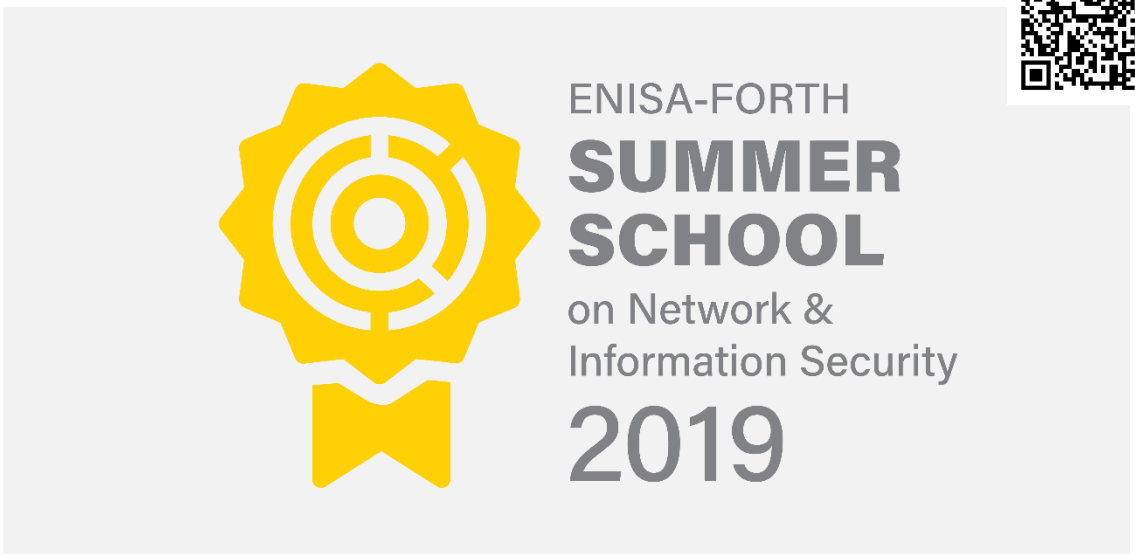
INSIKT_ En savoir plus sur les «Protocoles de certification en matière de renseignement sur la cybermenace».[22]

SANS_ FOR578: Cyber Threat Intelligence.[23]

FIRST.org_ Symposium sur le renseignement sur la cybermenace.[24]

Gov.uk_Cyber_ Formation au renseignement sur la menace (CRTIA).[25]

ENISA-FORTH_ Université d'été sur la sécurité des réseaux et des systèmes d'information – Formation au renseignement sur la cybermenace.[26]



Université d'été ENISA-FORTH 2019

Événement communautaire CTI-EU 2020

Aperçu

_Lacunes dans le matériel et les pratiques disponibles en matière de CTI

Bien que des niveaux de maturité plus élevés aient été atteints dans les pratiques et outils en matière de CTI ainsi que dans la fourniture et l'usage du CTI, il existe encore des lacunes dans ce domaine, en particulier en ce qui concerne différents cas d'utilisation, parmi lesquels le CTI sectoriel et les types de CTI (opérationnel, tactique, stratégique). Ces lacunes importantes ont été identifiées lors des discussions qui se sont tenues pendant le forum CTI de l'ENISA concernant la disponibilité de **renseignements sur la cybermenace actualisés et obtenus à partir d'attaques** sur des secteurs et services critiques. Il a été convenu que les éléments de CTI (par ex., les tactiques, techniques et procédures ou TTP) figurant dans diverses bonnes pratiques et cadres internationaux (par ex., ATT&CK[28]) devaient évoluer pour inclure des renseignements provenant d'un plus large éventail d'attaques. Les éléments de CTI relatifs à plusieurs secteurs ainsi qu'à différentes infrastructures et offres de prestation de services sont particulièrement urgents. Le manque d'intérêt accordé aux **attaques sur l'informatique en nuage** illustre bien cette situation.[29] Il est possible que des demandes similaires émanent d'infrastructures soit émergentes (par ex., la 5G[30]), soit spécialisées mais jouant un rôle essentiel dans des systèmes industriels critiques, notamment dans les systèmes de contrôle industriel (SCI) et dans les systèmes d'acquisition et de contrôle des données (SCADA).[31]

Bien que les cadres existants puissent contenir différents éléments utilisés dans les TTP pour cibler de tels systèmes, leur applicabilité dans plusieurs secteurs devra être élargie pour prendre en compte les particularités des TTP, telles que l'utilisation abusive des interfaces de programmation disponibles et l'exploitation des actifs principaux. Outre les TTP, les directives sur les **mesures de prévention, de détection et d'atténuation** relatives à ces secteurs font partie des éléments qui nécessiteront un examen plus approfondi.

Ces mesures faciliteront le développement des moyens nécessaires et permettront d'utiliser un CTI spécialement conçu pour ces secteurs. Pour différents types de plateformes et d'infrastructures, le principal obstacle à la diffusion d'un CTI exploitable est le délai qu'il existe entre la survenue d'un incident, la production d'un CTI connexe et l'intégration de ces informations dans des outils en open source. **Une coordination et une coopération plus étroites** entre les parties concernées permettront de réduire le délai avant la mise à disposition du CTI à l'ensemble des utilisateurs. Créer un climat de confiance entre les entités participantes est essentiel pour accélérer la chaîne d'approvisionnement du CTI. Pour faciliter ces interactions, il est important d'identifier des acteurs concernés et de mobiliser la communauté du CTI.

La disponibilité et la consommation de CTI dans le cadre de nombreuses activités liées à la gestion de la cybersécurité constituent un autre obstacle à l'établissement des capacités requises. Citons, par exemple, la gestion des crises de cybersécurité, la gestion des incidents, la réponse aux incidents, la chasse aux menaces et la gestion des vulnérabilités. Ces lacunes, déjà évaluées dans le précédent rapport sur le Paysage des menaces de l'ENISA (ETL)[32] au moyen de cycles asynchrones entre les différentes disciplines de la cybersécurité, persistent toujours.

Pour conclure cette section, il convient de noter que les lacunes décrites ne sont pas dues, en tant que telles, à un manque de connaissances en matière de CTI, mais plutôt aux longs cycles de communication et de coordination transsectoriels et intrasectoriels dans l'échange des connaissances du CTI.

Aperçu

_Problèmes émanant du développement d'une infrastructure de CTI

Le CTI est proposé dans certaines grandes catégories en fonction des besoins des utilisateurs en matière de CTI, besoins qui peuvent être opérationnels, tactiques ou stratégiques. Les offres commerciales actuelles qui proposent des outils de collecte, de maintenance, d'analyse et de diffusion de CTI, des sources d'informations de CTI, des plateformes de renseignement sur la menace (TIP - *Threat Intelligence Platform*), etc., répondent à quelques-uns de ces types de CTI. Cependant, il n'existe pas d'approche unique.

Les offres existantes sont axées sur le CTI opérationnel et tactique, tandis que le CTI stratégique est principalement proposé de manière indépendante.

Cependant, les frontières entre le CTI sont assez floues. Par conséquent, lorsqu'un consommateur de CTI souhaite mettre en place des moyens et l'environnement correspondant pour gérer le CTI, il n'est pas simple pour lui de sélectionner les éléments appropriés, ce qui s'explique principalement par le fait **que l'offre de services de CTI et le paysage des outils de CTI existants sont quelque peu fragmentés**. Pour tenter de créer un tel environnement, les utilisateurs de CTI devront sélectionner le meilleur système parmi les offres existantes. Leur sélection doit répondre aux exigences en matière de CTI ainsi qu'aux pratiques et processus de CTI appliqués, tout en tenant compte de leurs objectifs de maturité actuels et futurs en matière de CTI.

Bien que certains critères/exigences pour la sélection de TIP aient été élaborés[33] pour différents profils d'utilisateurs de CTI, des exigences similaires seront nécessaires pour d'autres produits, services et outils en matière de CTI. Dans l'idéal, ces exigences porteront sur différents niveaux de maturité des utilisateurs, différents niveaux de dépenses et différents types de CTI. Des critères/exigences similaires sont nécessaires pour plusieurs autres éléments d'une infrastructure CTI, comme les outils, les bonnes pratiques, les plateformes de partage, etc.

À long terme, OpenCTI[14] peut être une bonne solution pour résoudre les problèmes causés par la fragmentation des offres de CTI, étant donné sa capacité inhérente à intégrer des sources CTI de différents types dans un environnement d'outils unique.

Au cours de l'année à venir, les parties prenantes de l'ENISA et de la communauté du CTI s'efforceront d'évaluer les exigences en matière d'infrastructure de CTI et d'examiner comment les produits de CTI existants peuvent y répondre. Pour commencer, il faudra tenter d'établir une infrastructure de CTI répondant aux besoins internes de l'ENISA afin de développer une plateforme en vue d'obtenir un renseignement stratégique sur la cybermenace.

Aperçu

_Exploitation du CTI dans les disciplines connexes de la cybersécurité

L'intégration du CTI dans les disciplines clés de la cybersécurité a déjà été identifiée comme un enjeu par les membres de la communauté du CTI. C'est notamment le cas dans les activités et les composants de gestion de la sécurité liés à des environnements hautement dynamiques où l'exposition est accrue, comme les dispositifs d'utilisateur (par ex., les cartes USIM, les jetons d'authentification, les dispositifs mobiles, les systèmes industriels, les dispositifs de santé en ligne, etc.). Parmi les autres disciplines connexes pouvant bénéficier de manière significative du CTI figurent, entre autres, les activités de certification, les pratiques de gestion de crise, l'investigation numérique et la réponse aux incidents.

L'ENISA reconnaît[35] la nécessité d'**inclure le CTI dans le domaine de la certification**. En 2020, l'ENISA a créé un groupe de travail ad hoc visant à intégrer la gestion des risques et le CTI aux pratiques d'identification des niveaux d'assurance.

Le règlement sur la cybersécurité dispose notamment que ***«[l]e niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC ou processus TIC, en termes de probabilité et de répercussions d'un incident»*** **(article 52, paragraphe 1).**

Il est donc évident que le CTI doit s'inscrire dans le processus de certification à l'aide d'une évaluation du niveau d'assurance. Bien que certains éléments du CTI soient envisagés dans les normes de certification[36] en utilisant un «profil d'attaquant», ce concept comprend une faible part de CTI disponible.

Les travaux réalisés par **le groupe de travail ad hoc de l'ENISA** consiste à combiner les informations provenant des évaluations des risques et des menaces afin de regrouper de manière appropriée les exigences de protection et de les cartographier en fonction des différents niveaux d'assurance. La cartographie sera basée sur les différents niveaux de risque découlant de l'exposition des actifs à la menace et donnera lieu, simultanément, à des propositions concernant la quantité et l'intensité des contrôles d'atténuation. Ces contrôles permettront d'orienter la sélection des fonctions de sécurité qui seront attribuées à plusieurs niveaux d'assurance et qui seront mises en œuvre par les différentes cibles de certification.

Les travaux de l'ENISA sur le sujet sont réalisés avec le soutien d'un groupe d'experts qui rassemble des compétences en matière de gestion des risques, de CTI et de certification. Ces travaux ont commencé en avril 2020 et s'achèveront au troisième trimestre de la même année. L'ENISA en publiera les résultats.

Aperçu

_Résultats d'une enquête exhaustive sur le CTI

D'après une enquête représentative sur le CTI[7], il est possible de tirer plusieurs conclusions intéressantes sur l'utilisation actuelle des pratiques et des outils en matière de CTI. L'enquête reflète, entre autres, l'état actuel des capacités en matière de CTI, les types de CTI utilisés par les parties prenantes, l'interaction des pratiques de CTI avec d'autres processus au sein des organisations et les cas d'utilisation des outils de CTI.

Dans cette analyse, les résultats de l'enquête sont extrapolés aux expériences acquises par l'ENISA dans le cadre de ses propres activités (stratégiques) de CTI et aux commentaires des différentes parties prenantes de la communauté du CTI au sein de l'UE et des forums de CTI européens[36]. Dans ce contexte, l'accent est placé sur l'identification des besoins, la collecte d'informations, la production de CTI stratégique, l'utilisation d'outils et de pratiques ainsi que l'intégration dans d'autres processus pertinents. À cet égard, nous voudrions souligner les points ci-dessous.

- L'une des principales conclusions de ce rapport porte sur l'importance de disposer d'un outil de **semi-automatisation de la production de CTI**; tandis que l'ingestion de données automatisée est en hausse (malgré une augmentation de la consommation de CTI par les fournisseurs), les opérations manuelles constituent toujours la base de la production de CTI par les organisations.

- La gestion des opérations d'agrégation, d'analyse et de diffusion des informations s'effectue à l'aide **d'outils largement accessibles** tels que feuilles de calcul, courriels et plateformes de gestion open source, ce qui témoigne de l'efficacité des solutions à faible coût.

- L'importance de définir **des exigences en matière de CTI** est comprise par la communauté d'utilisateurs du CTI, ce qui répond aux appels répétés des experts du CTI[5,6] en faveur de la reconnaissance de l'importance des exigences en matière de CTI et montre que la communauté du CTI a suivi leurs conseils. Il est également intéressant de constater qu'un grand nombre d'exigences en matière de CTI reflète les besoins des entreprises et des dirigeants, ce qui indique que le CTI fait de plus en plus partie du processus décisionnel au niveau des entreprises et de la direction.
- La méthode la plus importante pour constituer une **base de connaissances interne en matière de CTI** consiste à combiner la consommation et la production de CTI. La tendance principale consiste à augmenter la production de CTI propre aux organisations, en particulier pour le CTI découlant de leur propre analyse des données brutes et des alertes de menace contextualisées. La consommation à partir de sources accessibles au public devient une tendance compte tenu de l'utilisation croissante de CTI disponible (flux CTI en open source, comme indiqué au point ci-dessous).
- **La collecte d'informations en open source** est la méthode d'ingestion la plus utilisée, suivie par les flux de menaces des fournisseurs de CTI. Il s'agit d'une nette tendance à la hausse en 2020, qui indique que les utilisateurs de CTI investissent dans leurs propres capacités pour concevoir un CTI conforme à leurs exigences.
- **La détection des menaces** est considérée comme le principal cas d'utilisation du CTI. Bien que les indicateurs de compromission restent les éléments les plus importants du CTI dans la détection des menaces et la réponse aux menaces, les comportements face aux menaces et les tactiques adverses (TTP) semblent expliquer les tendances à la hausse observées dans l'utilisation du CTI au sein des organisations.
- Mesurer l'**efficacité du CTI** est encore une tâche difficile; seul un faible pourcentage d'utilisateurs du CTI (4 %) mettent en œuvre des processus en vue d'en mesurer l'efficacité. Bien que les outils puissent apporter une valeur ajoutée à l'analyse du CTI, il n'en demeure pas moins que les compétences de l'analyste sont les plus importantes pour une mise en œuvre réussie du CTI. Concernant le niveau de satisfaction, il est intéressant de constater la faible note attribuée à la valeur des fonctions d'apprentissage automatique.

_Conclusions et prochaines étapes

Compte tenu de toutes ces évolutions dans le domaine du renseignement sur la cybermenace, il est possible de tirer les conclusions ci-dessous. Ces conclusions laissent apparaître certaines prochaines étapes, du moins du point de vue de l'ENISA, au cours desquelles elle renforcera le CTI conformément à son nouveau mandat, tout en tenant compte des évolutions observées dans ses communautés de parties prenantes, à savoir les États membres, la Commission européenne et d'autres organismes européens, les fournisseurs et les utilisateurs finaux du CTI:

- Étant donné le nombre croissant de parties prenantes dans l'UE et dans les États membres, **la coopération et la coordination des activités du CTI à l'échelle de l'UE** sont primordiales. Si la mise en place de synergies peut réduire les coûts du CTI, elle permet également de renforcer la confiance entre ses acteurs, permettant ainsi le partage de renseignements sur la cybermenace et de bonnes pratiques. L'ENISA encouragera la coopération avec les différentes parties prenantes en lançant **l'identification des exigences en matière de CTI.** Cette coopération comprendra de multiples groupes de parties prenantes au sein de l'écosystème des organisations de l'UE (c.-à-d. la Commission, les organes, agences et États membres de l'UE).
- La pertinence du CTI pour la prise de décisions stratégiques et politiques étant entendue, il importe de **faciliter sa connexion avec les informations géopolitiques et les systèmes cyberphysiques**, ce qui permettra d'intégrer le CTI dans les processus décisionnels, mais aussi d'élargir son cadre à l'identification des menaces hybrides.

- **L'intégration du CTI aux processus de gestion de la sécurité** aidera le CTI à proliférer dans des domaines connexes et contribuera à l'identification, la détection et la prévention des menaces en temps utile. L'une des retombées immédiates sera l'amélioration de la flexibilité de processus relativement longs (par ex., la certification, l'évaluation des risques). En même temps, le CTI facilitera la prise de décisions d'urgence (par ex., la gestion de crise) en fournissant des preuves de l'exposition aux cybermenaces.
- Pour mieux répondre au rôle croissant du CTI, l'ENISA œuvrera à **l'élaboration d'un programme global en matière de CTI**. Le programme de CTI de l'ENISA regroupera horizontalement les compétences internes afin d'inscrire l'ensemble des parties prenantes concernées dans toutes les phases de production et de diffusion du CTI et de développer une infrastructure CTI qui sera utilisée tant pour des besoins internes qu'à des fins de formation.
- L'investissement dans certains concepts de base du CTI, en particulier **sa maturité et la hiérarchie des menaces**, est considéré comme très utile pour augmenter l'utilisation du CTI. En collaboration avec ses partenaires de l'UE, l'ENISA s'efforcera de développer un modèle de maturité pour le CTI. En outre, l'ENISA consolidera et diffusera du contenu CTI multifonctionnel et utile, tel que la hiérarchie des menaces utilisable dans d'autres domaines (par ex., la certification, la gestion des risques, les paysages sectoriels, etc.).

Certaines des conclusions et prochaines étapes susmentionnées feront l'objet de travaux de l'ENISA dans le domaine du CTI au cours des prochaines années.[35]

Références

1. «Cyber Threat Intelligence Lab» HPI et TU Delft. https://www.cyber-threat-intelligence.com/

2. «5-Step process to power your Cyber Defense with Cyber Threat Intelligence». 12 mars 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». 3 septembre 2019. SANS, https://www.youtube.com/watch?v=J7e74QLVxCk

4. «Maturing Cyber Threat Intelligence». HPI et 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». 20 mars 2019. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. «2020 SANS Cyber Threat Intelligence (CTI) Survey». 10 février 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». 9 septembre 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». 25 octobre 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

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

11. «Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts». Mars 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». 15 janvier 2020. Recorded Future. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

13. «A List of the Best Open Source Threat Intelligence Feeds». 4 mars 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». 16 mars 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». 11 décembre 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». Janvier 2020. NetScope. https://www.enisa.europa.eu/events/2019-cti-eu/presentations/the-cti-cloud-context-dilema

30. «ENISA Threat Landscape for 5G Networks». Octobre 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

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

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

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

34. «ENISA Programming Document». Novembre 2019. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

35. «Règlement de l'UE sur la cybersécurité» 7 juin 2019. Journal officiel de l'Union européenne. https://eur-lex.europa.eu/legal-content/FR/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

Documents connexes

Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Liste des 15 principales menaces**

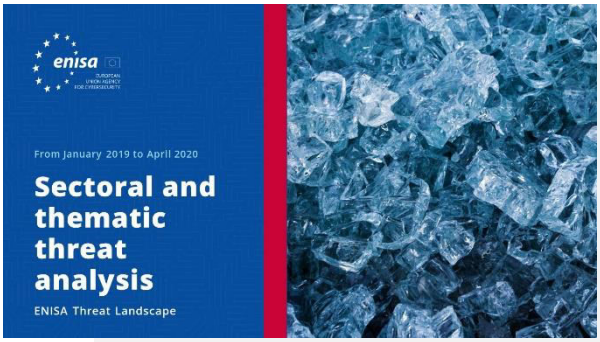
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Thèmes de recherche**

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.

LIRE LE RAPPORT



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Principaux incidents dans l'UE et dans le monde**

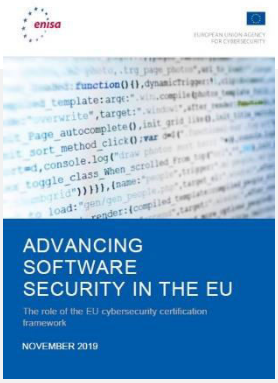
Principaux incidents de cybersécurité survenus entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

Autres publications



Advancing Software Security in the EU

Ce rapport présente les éléments clés de la sécurité logicielle et donne un bref aperçu des approches et des normes existantes les plus pertinentes dans le paysage du développement de logiciels sécurisés.

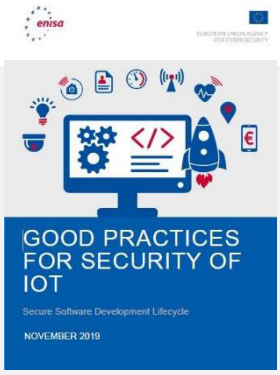
LIRE LE RAPPORT

ENISA good practices for security of Smart Cars

Bonnes pratiques pour la sécurité des voitures intelligentes, c'est-à-dire les véhicules connectés et (semi-)autonomes, afin d'améliorer l'expérience des utilisateurs et la sécurité des voitures

.

LIRE LE RAPPORT



Good Practices for Security of IoT - Secure Software Development Lifecycle

Sécurité de l'internet des objets mettant l'accent sur les orientations en matière de développement logiciel.

LIRE LE RAPPORT

«La pertinence du CTI pour la prise de décisions stratégiques et politiques étant entendue, il importe de faciliter sa connexion avec les informations géopolitiques et les systèmes cyberphysiques»

ETL 2020

À propos

L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site https://www.enisa.europa.eu/media/enisa-en-francais/.

Contributeurs

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

Éditeurs

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

Contact

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

Nous aimerions avoir votre avis sur ce rapport!
Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer ici.

Avis juridique

Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

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

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu