FR

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De janvier 2019 à avril 2020

Thèmes de recherche

Paysage des menaces de l'ENISA

Aperçu

Grâce aux activités de recherche et d'innovation menées par des universitaires, des industriels et des professionnels du monde entier, on assiste à une émergence de nouveaux concepts et de nouvelles idées dans le domaine de la cybersécurité. Il s'agit là d'étapes importantes car la vitesse des adversaires (c.-à-d. les acteurs malveillants) à innover est plus élevée que celle des spécialistes de la cybersécurité à trouver des solutions pour les dissuader d'agir. En effet, outre l'hygiène et la formation de base en matière de cybersécurité, investir dans la recherche et l'innovation est l'option la plus viable pour permettre aux défenseurs de se rapprocher de ce qu'il faut faire pour améliorer la sécurité du cyberespace. Dans le présent rapport, nous mettrons en évidence certains des thèmes de recherche et d'innovation en matière de cybersécurité les plus importants parmi ceux qui ont été explorés dans l'UE et dans le monde.

Meilleure compréhension de la dimension humaine

La cybersécurité est toujours considérée comme la pratique qui consiste à protéger les réseaux, les systèmes d'information et les données. Il est nécessaire d'élargir cette définition au-delà des aspects techniques pour y inclure les préoccupations sociales, comportementales et économiques ainsi que les différents rôles joués par les parties concernées. Telle devra être la priorité dans les débats futurs qui porteront sur la recherche et l'innovation en matière de cybersécurité. Pour définir une stratégie de cybersécurité, il est essentiel d'avoir une meilleure compréhension de la dimension humaine afin que les décisions en matière de sécurité soient prises en fonction des besoins, des compétences et des attentes de chacun.

Recherche et innovation en matière de cybersécurité

En 2019, nous avons constaté une augmentation du nombre de laboratoires d'essai et de *cyber ranges*[1] mis à disposition sur site et proposés en ligne. Il s'agit là de ressources essentielles qui permettent aux chercheurs de simuler des attaques, d'élaborer des scénarios d'exploitation, d'obtenir des données opérationnelles et de tester des stratégies de défense dans un environnement virtuel polyvalent. Toutefois, les environnements d'essai existants ne suffisent pas à reproduire les nombreuses vulnérabilités qui compromettent généralement la sécurité, notamment les facteurs humains et techniques. Pour améliorer l'efficacité, il importe de poursuivre la recherche et l'innovation en se focalisant sur la portée et la précision de ces laboratoires d'essai et de proposer de nouvelles solutions techniques.

Aperçu

La sécurité 5G

Dans certains pays, le déploiement des réseaux mobiles 5G a débuté en 2019, mais on s'attend à ce que le nombre d'installations augmente en 2021. Cette nouvelle génération de communications mobiles revêt une importance capitale pour le progrès économique et social de l'Union européenne. Par conséquent, les futurs travaux de recherche et développement relatifs aux solutions de sécurité 5G sont cruciaux pour garantir la durabilité et la fiabilité de cette technologie. En 2019, l'ENISA a publié un paysage des menaces pour les réseaux 5G, passant en revue certains aspects critiques de la sécurité liés à cette technologie émergente.[2] Les principaux thèmes de recherche et d'innovation en matière de sécurité 5G doivent tenir compte des aspects énoncés ci-dessous.

- La recherche et le développement de contrôles de sécurité pour couvrir la protection du réseau, des éléments physiques et des couches de données, offrant ainsi une solution de protection multicouche. Avec les réseaux 5G, les données seront stockées sur des serveurs en nuage centralisés, des nœuds de brouillard intermédiaires et des dispositifs de bord, ce qui rendra plus complexe la mise en œuvre d'une solution de sécurité.

- La recherche et le développement de normes et d'exigences pour les contrôles de sécurité à mettre en œuvre sur des réseaux interconnectés ayant de multiples propriétaires, topologies, opérateurs et une diversité de dispositifs et de couches réseau.

- La recherche et le développement de capacités de gestion de clés permettant une interopérabilité sécurisée entre les nœuds connectant des dispositifs à ressources limitées et des dispositifs de l'internet des objets. Cette capacité doit inclure des techniques efficaces de contrôle d'accès, d'authentification, de cryptographie et de gestion de clés pour les nœuds à ressources limitées.

Les projets de recherche et d'innovation de l'UE sur la cybersécurité

- L'UE œuvre à la mise en place d'un pilote pour la création d'un réseau de compétences en cybersécurité. CONCORDIA[3], ECHO[4], SPARTA[5] et CyberSec4Europe[6] sont les quatre projets pilotes gagnants de l'appel à propositions sur la cybersécurité d'Horizon 2020 lancé en 2018 pour «établir et exploiter un pilote pour un réseau de compétences en cybersécurité en Europe visant à élaborer une feuille de route commune pour la recherche et l'innovation dans la cybersécurité européenne». Pour garantir un marché unique numérique plus sûr en Europe, l'UE compte renforcer ses capacités en matière de cybersécurité et relever les défis futurs dans ce domaine grâce à ces quatre projets pilotes.
- L'UE accorde 38 millions d'euros pour la protection des infrastructures critiques contre les cybermenaces. La Commission européenne a annoncé qu'elle débloquerait plus de 38 millions d'euros dans le cadre d'Horizon 2020 pour le programme de recherche et d'innovation de l'UE. Ce programme vise à soutenir plusieurs projets innovants dans le domaine de la protection des infrastructures critiques contre les cybermenaces et menaces physiques ainsi qu'à rendre les villes plus intelligentes et plus sûres.[7]
- L'UE a lancé un appel à projets de 10,5 millions d'euros dans le domaine de la cybersécurité. La Commission a lancé un nouvel appel d'une valeur de 10,5 millions d'euros dans le cadre du programme «Connecting Europe Facility» (CEF) pour des projets visant à renforcer les capacités européennes et la coopération entre les États membres en matière de cybersécurité.[8]

Recherche et innovation en matière de CTI

Diffusion rapide des méthodes et du contenu du CTI

Au cours de la période considérée, différents besoins de recherche ont été identifiés et les actions visant à répondre à ces besoins sont proposées ici. Ces actions ont été regroupées en plusieurs catégories afin de mieux refléter leur portée. Bien qu'elles puissent se recouper, ces catégories sont indicatives des domaines dans lesquels le CTI pourrait être amélioré.

- **Les résultats des projets de recherche dans le domaine du CTI doivent être évalués et cartographiés dans un contexte plus large** afin d'identifier les chevauchements et les lacunes, puis de les comparer aux pratiques, services et produits commerciaux existants en matière de CTI. La diffusion des résultats à la communauté d'utilisateurs sera ainsi facilitée. Parallèlement, les lacunes existantes seront comblées par l'ajout de fonctions, de contenu et de processus. Les projets de l'UE (Horizon H2020) présentant un intérêt pour le CTI sont d'excellents atouts pour cette tâche, car ils contribuent à améliorer les pratiques en matière de CTI.
- **La fourniture et l'utilisation de matériel de CTI en open source doivent être encouragées.** Le transfert des connaissances sera ainsi facilité et le seuil de compétences réduit en matière de CTI. À cet effet, la plateforme OpenCTI est la solution idéale car elle permet d'intégrer des renseignements sur la cybermenace tirés de multiples sources dans une seule base, qui peut ensuite être partagée entre différents utilisateurs, tout en offrant un ensemble de fonctions pour la gestion de ces informations. En se dotant d'OpenCTI, les utilisateurs seront en mesure d'obtenir de précieuses informations avec un seuil de compétences relativement bas.

_Recherche donnant lieu à des tendances émergentes

La nécessité de **renforcer le CTI** au moyen d'autres outils de cybersécurité établis exige que ce domaine évolue d'un point de vue structurel et contextuel. Simultanément, les progrès techniques rendus possibles grâce aux nouvelles technologies posent la question de savoir comment le CTI peut bénéficier de ces développements. Ainsi, les besoins en **recherche prospective** dans le domaine du CTI contribueront à améliorer les processus, les fonctions, l'automatisation, la structure et la validation des contenus, la prestation de services, le débit vers l'utilisateur/de diffusion, le déploiement et les projections du CTI.

Le renseignement sur la cybermenace s'est imposé dans le domaine de la cybersécurité comme un outil essentiel pour améliorer la flexibilité et l'efficacité de la défense contre les cyberattaques.

Recherche et innovation en matière de CTI

Fonctionnalité, niveau d'automatisation et conformité aux exigences de maturité

- **L'automatisation des processus jouera un rôle clé dans le CTI**. Alors que les cyberattaques modernes sont désormais fortement automatisées, les organisations essaient de se défendre manuellement ou en n'utilisant que partiellement l'automatisation contre celles-ci. Il s'agit d'un combat inégal qui ralentit la vitesse et la capacité de réaction. Il sera essentiel d'étudier la possible automatisation des processus de CTI pour parvenir à un équilibre entre les attaquants et les défenseurs. Pour ce faire, il faudra procéder à une analyse approfondie des étapes relatives aux processus du CTI et des possibilités d'automatisation de ces étapes au moyen des technologies disponibles et émergentes.
- **Les exigences de maturité du CTI devront être définies plus en détail**. Bien que certains critères/exigences pour la sélection des fonctions du CTI (par ex., les plateformes d'analyse de la menace, ou TIP pour *Threat Intelligence Platforms*) aient été élaborés pour différents profils d'utilisateurs du CTI, des exigences similaires seront nécessaires pour d'autres produits, services et outils en matière de CTI. Ces exigences seront associées à plusieurs niveaux de maturité et de dépenses des utilisateurs ainsi qu'à plusieurs types de CTI. Des critères/exigences similaires sont nécessaires pour divers autres éléments d'une infrastructure CTI, tels que les outils, les bonnes pratiques, les plateformes de partage, etc. Par conséquent, outre le développement de modèles de maturité des capacités du CTI, des recherches sont nécessaires pour montrer à quel point les fonctions du CTI correspondent à ses différents niveaux de maturité. Ces travaux contribueront à accélérer l'adoption des pratiques de CTI.
- **L'utilisation de l'intelligence artificielle/apprentissage automatique dans le CTI doit faire l'objet d'une étude plus approfondie**, ce qui permettra de réduire le nombre d'étapes manuelles dans l'analyse du CTI et augmentera la valeur des fonctions d'apprentissage automatique au sein des activités de CTI.

Création de passerelles vers des domaines connexes

- Il convient de développer de **nouvelles approches pour l'ingestion des connaissances du CTI en fonction de domaines** pouvant en bénéficier. Les *cyber ranges*, les menaces hybrides, les chaînes d'approvisionnement ainsi que les évaluations et crises géopolitiques en sont des exemples. Les questions à se poser à cet égard sont les suivantes: Quels sont les points pour lesquels le CTI peut être pris en compte? Quel est le contenu du CTI pertinent? Quels sont les critères de validation de la pertinence des informations du CTI? Comment le CTI peut-il être «connecté» aux informations sur le domaine concerné? Quel type d'informations provenant de ces domaines peut être ajouté au CTI? Les synergies auxquelles renvoient ces questions peuvent favoriser les cas d'utilisation et la qualité du contenu de manière omnidirectionnelle.

- **Le CTI est essentiel pour un certain nombre de disciplines**. Citons notamment l'évaluation/la gestion des risques, la définition des exigences de protection et la certification. Ces disciplines tireront profit d'une utilisation correcte du CTI. Il est possible d'identifier la contribution du CTI à ces disciplines en ayant recours à des informations telles que les modèles de menace, les renseignements sur les acteurs malveillants (capacités, motifs), les méthodes d'attaque et les codes d'exploitation. Bien que du contenu pertinent existe déjà (par ex., le cadre MITRE ATT&CK[2]), un travail considérable reste à accomplir pour pouvoir identifier et normaliser ces interfaces d'informations.

Recherche et innovation en matière de CTI

Efficacité des opérations du CTI

- **Les méthodes permettant d'utiliser efficacement le CTI serviront à la prise de décision.** Ces méthodes de déploiement efficace du CTI aideront les décideurs à comprendre la valeur du CTI et les praticiens à en évaluer le retour sur investissement. Ces méthodes/ICP devront tenir compte de facteurs allant au-delà du contenu du CTI, en prenant en considération les améliorations obtenues au cours du cycle de vie complet de la gestion de la sécurité et de l'atténuation des risques. De façon optimale, la mesure de l'efficacité des investissements dans le CTI s'inscrira dans le cadre d'une réflexion beaucoup plus large sur l'économie de la cybersécurité dans différents types d'organisations (par ex., en fonction des exigences de sécurité, des niveaux de maturité, etc.).

- Bien que des outils peu coûteux prévalent pour l'agrégation, l'analyse et la diffusion du CTI, **quelques recherches peuvent s'avérer nécessaires pour trouver des outils automatisés afin de gérer le CTI** consommé et produit. Outre les formats de données standard (par ex., les fichiers CSV, STIX, TAXII), les fonctions CTI standard peuvent faire l'objet de telles recherches, qui seront suivies par le développement d'outils peu coûteux, en open source, qui prendront en charge ces fonctions.

Évolution de la structure et du contenu du CTI

- Au fur et à mesure de la pénétration du CTI dans d'autres domaines, **les informations issues de ces contextes doivent être transmises à la base de connaissances d'origine du CTI**. Les structures du CTI doivent notamment être définies afin de recueillir des informations sur les menaces géopolitiques et hybrides. Il en va de même pour la pertinence du CTI en ce qui concerne les risques, les incidents, les analyses criminalistiques, les niveaux d'assurance, etc. Les formats actuels du CTI doivent évoluer afin de recueillir des informations émanant de ces éléments.

- **Les technologies émergentes comme l'intelligence artificielle (IA)** peuvent être utilisées pour valider le CTI analysé. Ces outils peuvent compléter, voire remplacer, l'analyse manuelle du CTI, mais également fournir un soutien tout au long du cycle de vie du CTI (par ex., en vérifiant la pertinence du CTI en fonction des informations existantes sur les incidents). Ces nouvelles approches en matière de CTI amélioreront la qualité et la pertinence des informations.

Références

1. Le concept de *cyber range* a été défini pour la première fois en 2013 par l'Agence européenne de défense (AED), dans le rapport intitulé « *Common staff target for military cooperation on cyber ranges in the European Union* », comme un environnement polyvalent à l'appui de trois processus primaires: le développement, la garantie et la diffusion des connaissances.

2. «ENISA threat landscape for 5G Networks». 21 novembre 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

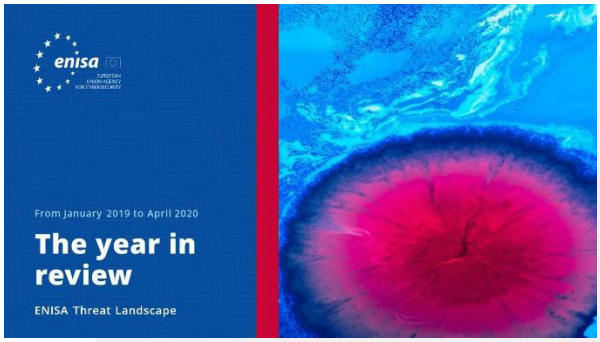
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

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

«Le renseignement sur la cybermenace (CTI) s'est imposé dans le domaine de la cybersécurité comme un instrument essentiel pour améliorer la flexibilité et l'efficacité de la défense contre les cyberattaques.»

ETL 2020

Documents connexes



LIRE LE RAPPORT

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

Résumé des principales tendances de l'année en matière de cybersécurité.

LIRE LE RAPPORT

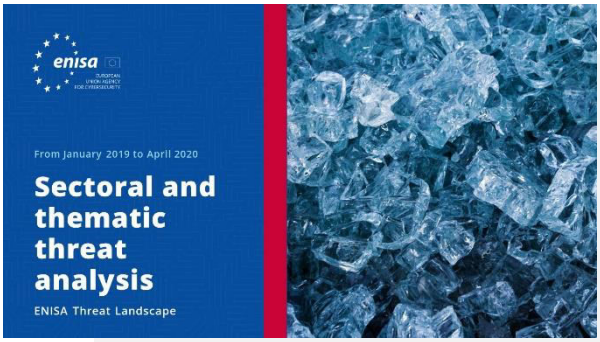
Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

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 **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 **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 **Tendances émergentes**

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

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Aperçu du renseignement sur la cybermenace

L'état actuel du renseignement sur la cybermenace dans l'UE.

Autres publications

Roadmap on the Cooperation Between CSIRTS and LE

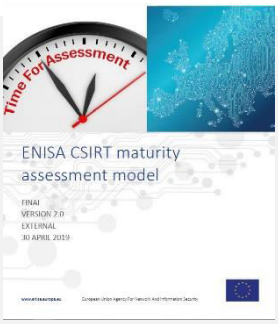
Feuille de route sur la coopération entre les CSIRT, en particulier avec les forces de l'ordre nationales et gouvernementales et le système judiciaire.

LIRE LE RAPPORT

EU MS Incident Response Development Status Report

Étude visant à analyser le dispositif opérationnel actuel de réponse aux incidents dans les secteurs concernés par la directive NIS et à identifier les changements récents.

LIRE LE RAPPORT



ENISA CSIRT maturity assessment model

Version actualisée du document «Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity» publiée par l'ENISA en 2017

LIRE LE RAPPORT

«La sophistication des capacités de menace s'est accrue en 2019; de nombreux adversaires ont désormais recours aux codes d'exploitation, au vol d'identifiants et aux attaques en plusieurs étapes.»

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