enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

EN

De enero de 2019 a abril de 2020

Sinopsis de la inteligencia sobre las ciberamena

Sinopsis

_Desarrollos en el área de la CTI

En este informe se **evalúa la situación en la que se encuentra la inteligencia sobre las ciberamenazas (cyber threat intelligente, CTI) como dominio dinámico de la ciberseguridad**. El objetivo de este análisis es indicar las tendencias principales en el rápido desarrollo de la CTI proporcionando referencias relevantes y resumiendo los pasos siguientes necesarios para avanzar en este tema durante los próximos años.

En enero de 2020, la ENISA organizó su evento **CTI-EU**[2] que tiene como objetivo fortalecer la relación entre los integrantes de este colectivo. En este evento hubo varias presentaciones que demostraron la situación actual de la CTI en los ámbitos comercial, institucional y de usuario. Las presentaciones, debates y demostraciones de proveedores de CTI abordaron el estado de los productos, enfoques y prácticas e indicaron los problemas existentes. Es evidente que la **CTI ha conseguido una madurez suficiente y ya se dispone de una masa crítica de** material relacionado con este tema, p. ej., a través de las prácticas actuales, herramientas y procesos.

Parece que el **próximo reto en CTI será digerir, consolidar y difundir las prácticas existentes** para conseguir hacer un uso más amplio de una forma rentable y sinérgica. Las oportunidades principales en este respecto se encuentran en compartir prácticas, requisitos, herramientas e información de CTI de forma no competitiva. Asimismo, la identificación de las nuevas partes interesadas que entran en el campo de la CTI –productores y consumidores– mejorarán las capacidades, identificarán requisitos de CTI y establecerán medios para compartir la inteligencia de forma oportuna. La ENISA planea reforzar las sinergias y difundir buenas prácticas en materia de CTI tanto a través del evento CTI-EU como de la cooperación con varias partes interesadas de la UE.

_Herramientas, material y prácticas de CTI

Comisión del programa marco de investigación e innovación Horizonte 2020_ En H2020 se han completado varios proyectos relacionados con la CTI o se encuentran aún en curso. Ya han consumido una cantidad importante de fondos y han dado como resultado varias herramientas y prácticas para producir, consumir y usar la CTI.

Prácticas de los órganos de normalización, organizaciones internacionales, administraciones, industria, universidades y usuarios particulares_ Se ha desarrollado un conjunto de buenas prácticas que cubren: métodos de CTI, temas sobre la madurez de los marcos de trabajo y de los modelos de procesos[1,2,3], requisitos, encuestas de uso, evaluación de herramientas[8,9,10], enfoques para el desarrollo de la CTI[11,12], etc.

Ofertas de CTI abiertas_ Para los productores y consumidores disponer de varias fuentes y herramientas públicas[13] que respalden OpenCTI[14] es importante, ya que permiten el acceso gratuito a conocimientos valiosos de CTI a bajo coste.

Herramientas (y prácticas) de CTI abiertas_ Se han presentado numerosas herramientas, prácticas y artículos[15,16] que proporcionan enfoques prácticos para el análisis de la CTI y su difusión mediante herramientas gratuitas.[17,18,19]

Sinopsis

_Oportunidades de formación en materia de CTI

CYBRARY_ Introducción a la inteligencia sobre las ciberamenazas.[21]

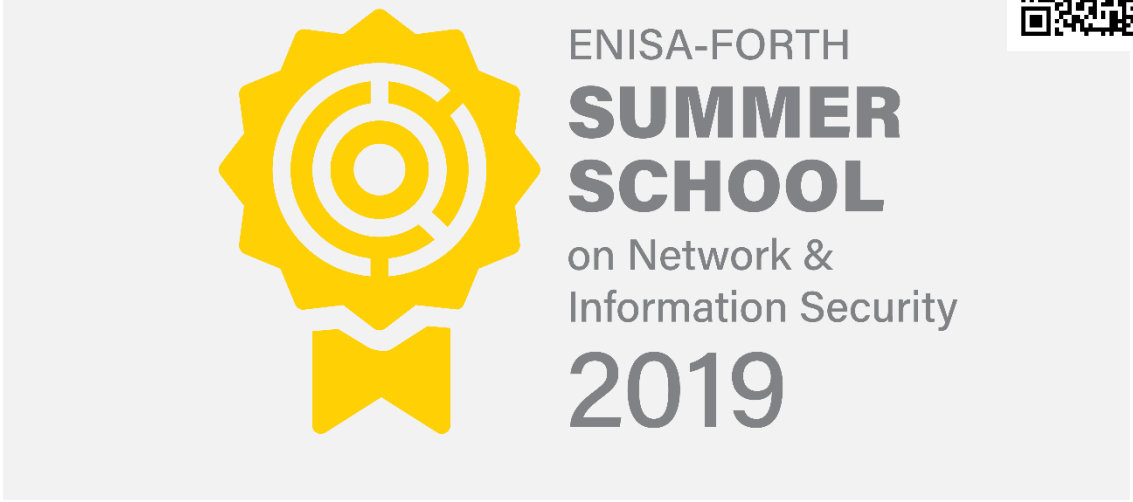
INSIKT_ Aprender más sobre los «protocolos de certificación de inteligencia sobre las ciberamenazas».[22]

SANS_ FOR578: Inteligencia sobre las ciberamenazas.[23]

FIRST.org_ Simposio de Inteligencia sobre las ciberamenazas.[24]

Gov.uk_Cyber_ Formación en inteligencia sobre las amenazas (CRTIA).[25]

ENISA-FORTH_ NIS (*Network and Information Security*, seguridad de las redes y de la información). Curso de verano: formación en Inteligencia sobre las ciberamenazas.[26]



CUARTO Curso de verano de la ENISA 2019

Evento comunitario CTI-EU 2020

Sinopsis

_Lagunas en el material y prácticas disponibles sobre CTI

A pesar de lo altos niveles de madurez logrados en las prácticas y herramientas de CTI, y la provisión y consumo relacionados con este tema, aún existen lagunas, especialmente las relacionadas con varios casos de uso, CTI por sectores y tipos de CTI (operativo, táctico, estratégico), entre otras. Estas importantes lagunas se han identificado en conversaciones con el foro de CTI de la ENISA sobre la disponibilidad de **CTI actualizada proveniente de ataques** en sectores y servicios vitales. Se ha acordado que elementos de la CTI, p. ej., los TTP (tácticas, técnicas y procedimientos), incluidos en varios marcos de trabajo y buenas prácticas internacionales (p. ej., ATT&CK[28]) deben evolucionar para incluir inteligencia proveniente de un espectro de ataques más amplio. Los elementos de CTI de varios sectores e infraestructuras de provisión de servicios y ofertas son particularmente urgentes. Un ejemplo de esto es la poca atención que se presta a los **ataques a la computación en la nube**.[29] Podrían surgir solicitudes similares de las infraestructuras emergentes (p. ej., 5G[30]) o de naturaleza especializada, pero que desempeñan una función esencial en los sistemas industriales vitales, por ejemplo en los sistemas de control industrial (ICS) o en los de control de supervisión y adquisición de datos (SCADA).[31]

Aunque los marcos de trabajo existentes pueden contener varios elementos utilizados en los TTP dirigidos a esos sistemas, su aplicabilidad en varios sectores tendría que ampliarse para incluir las peculiaridades de estos TTP, como el abuso de las interfaces de programación de aplicaciones (API) disponibles y la explotación de los recursos principales. Aparte de los TTP, otros elementos que requerirán más consideración son las directrices para las **prácticas de prevención, detección y mitigación** para estos sectores.

Esto facilitará el desarrollo de las capacidades necesarias y permitirá el uso de una CTI especialmente diseñada para estos sectores. La barrera principal para la difusión de una CTI práctica para varios tipos de plataformas e infraestructuras es el lapso de tiempo entre un incidente, la recopilación de la CTI relacionada y la difusión de esta información a las herramientas de código abierto. **Una coordinación y una cooperación más estrechas** entre las partes involucradas reduciría el tiempo que se tarda en distribuir la CTI al resto de los usuarios. Crear un clima de confianza entre las entidades participantes es la clave para acelerar la cadena de suministro de CTI. La identificación de los participantes relevantes y la movilización de la comunidad de CTI también son elementos importantes para facilitar estas interacciones.

Otra barrera para conseguir las capacidades necesarias es la disponibilidad y consumo de CTI en varias actividades de gestión de la ciberseguridad. Como ejemplos se podrían citar la gestión de las crisis de ciberseguridad, la gestión de incidentes, la respuesta ante incidentes, la búsqueda de amenazas y la gestión de la vulnerabilidad. Esta deficiencia se evaluó en el informe Panorama de amenazas de la ENISA (PAE)[32] anterior mediante ciclos asíncronos entre las disciplinas de ciberseguridad y aún persiste.

Para concluir este apartado cabe mencionar que las deficiencias descritas no se deben a la falta de conocimiento en materia de CTI de por sí, sino a los largos ciclos de comunicación tanto intersectoriales como intrasectoriales para el intercambio de información de CTI.

Sinopsis

_Temas emergentes en la creación de la infraestructura de CTI

La CTI se ofrece en algunas categorías amplias según los requisitos de los usuarios en esta materia, principalmente operativos, tácticos y estratégicos. La oferta comercial existente de herramientas para la recopilación, mantenimiento, análisis y difusión de CTI, canales de CTI, plataformas de inteligencia sobre las amenazas (threat intelligence platforms, TIP), etc., respaldan algunos de estos tipos de CTI. Sin embargo, no hay un enfoque que sirva para todos.

Las ofertas existentes se concentran en la CTI operativa y táctica, mientras que la CTI estratégica se ofrece principalmente de forma independiente.

Aun así, los límites entre las CTI son bastante difusos. Esto hace que, cuando un consumidor de CTI quiere aumentar una capacidad y el entorno correspondiente para gestionar la CTI, no le sea fácil seleccionar los elementos adecuados. Esto se debe principalmente a que la **provisión de servicios de CTI y el panorama de herramientas existentes para esta materia están bastante fragmentados**. Cuando se intenta construir un entorno de este tipo, los usuarios de CTI necesitarán hacerlo seleccionando el mejor sistema a partir de la oferta existente. La selección tiene que cubrir los requisitos de CTI y las prácticas y procesos aplicados en esta materia, y a la vez tener en cuenta la madurez de los objetivos actuales y futuros de CTI.

Aunque se han desarrollado algunos criterios y requisitos para seleccionar TIP[33] para diversos perfiles de usuario de CTI, será necesario establecer requisitos similares para desarrollar más productos, servicios y herramientas para esta disciplina. Lo ideal sería que dichos requisitos se centraran en los diversos niveles de madurez del usuario, niveles de gasto y tipos de CTI. Es necesario utilizar criterios o requisitos similares para el resto de los elementos de la infraestructura de CTI, como las herramientas, las buenas prácticas, el uso compartido de plataformas, etc.

A largo plazo, parece que OpenCTI[14] podría ser una buena solución para resolver los problemas causados por la fragmentación de la oferta de CTI, dada su capacidad inherente para integrar fuentes de CTI de varios tipos en un único entorno de herramientas.

El próximo año la ENISA y las partes interesadas de CTI dedicarán sus esfuerzos a evaluar los requisitos de la infraestructura para esta materia y ver cómo pueden cubrirlos los productos ya existentes. Este trabajo empezará con un intento de establecer una infraestructura de CTI para las necesidades internas de la ENISA para el desarrollo de una plataforma de inteligencia para la CTI de tipo estratégico.

Sinopsis

_Aprovechamiento de la CTI de disciplinas de ciberseguridad relacionadas

Los miembros de la comunidad de CTI ya han identificado la incorporación de la CTI entre las disciplinas de ciberseguridad claves como un tema relevante. Es especialmente el caso de las actividades y componentes de gestión de la seguridad relacionados con entornos muy dinámicos y con una exposición alta, como los dispositivos de los usuarios (p. ej., módulos de identidad de abonados [USIMS], *tokens* de seguridad, dispositivos móviles, sistemas industriales, dispositivos de salud electrónicos, etc.). Otras disciplinas relacionadas que podrían beneficiarse de forma significativa de la CTI son las actividades de certificación, las prácticas de gestión de crisis, la informática forense y la respuesta ante incidentes, entre otras.

La ENISA es consciente[35] de la necesidad de la **incluir la CTI en el área de las certificaciones**. En 2020, la ENISA estableció un grupo de trabajo específico cuyo fin era integrar la gestión de riesgos y la CTI con prácticas para identificar los niveles de garantía.

Concretamente, la CSA declara que ***«El nivel de garantía debe ser proporcional al nivel de riesgo asociado al uso previsto del producto, servicio o proceso de CTI, en términos de probabilidad e impacto de un incidente»*** **(Art. 52(1)).**

Esto demuestra que la CTI tiene que desembocar en el proceso de certificación usando una evaluación del nivel de garantía. Aunque hay partes de la CTI que se han considerado en los estándares de certificación[36] usando un «perfil de atacante», este concepto solo engloba una pequeña parte de la CTI disponible.

El trabajo realizado por el **grupo de trabajo específico de la ENISA** consiste en combinar la información de las evaluaciones de riesgos y amenazas (CTI) con los requisitos de protección de grupo apropiados y asociarlos a varios niveles de garantía. Esta asociación se basará en los varios niveles de riesgo que emergen de la exposición de los activos a la amenaza y, a la vez, dará lugar a propuestas sobre el número y fortaleza de los controles de mitigación. Estos controles dirigirán la selección de las funciones de seguridad que se asignarán a varios niveles de garantía y que estarán sujetos a ser implementados por los diversos objetivos de certificación (targets of certification, ToC).

El trabajo de la ENISA en esta materia se está realizando con el apoyo de un grupo de expertos con una combinación de capacidades de gestión de riesgos, CTI y certificación. El trabajo empezó en abril de 2020 y concluirá en el tercer trimestre de 2020. La ENISA publicará los resultados de este trabajo.

Sinopsis

Resultados de una encuesta exhaustiva sobre la CTI

A partir de una encuesta representativa sobre la CTI[7], se han podido extraer varias conclusiones de interés sobre la asimilación actual de las prácticas y herramientas relacionadas con esta disciplina. Entre otros temas, la encuesta refleja el estado actual de las capacidades de CTI, los tipos de CTI utilizados, los tipos de CTI utilizados por las partes interesadas, la interacción de las prácticas de CTI con otros procesos en organizaciones y los casos de uso de las herramientas de CTI.

En este análisis se extrapolan los resultados de la encuesta a las experiencias ganadas por la ENISA con sus propias actividades de CTI (estratégicas) y los comentarios de varias de las partes interesadas en esta materia de la UE y de los foros de CTI europeos[36]. En este contexto, el foco se dirige a la identificación de requisitos, la recopilación de información, la producción de CTI estratégica, el uso de herramientas y prácticas, y la integración con otros procesos relevantes. A este respecto, deseamos destacar los puntos siguientes:

- Una de las conclusiones principales de este informe es que la **semiautomatización de la producción de CTI** es una herramienta importante: aunque la automatización del consumo de información va en aumento (a pesar del aumento en el consumo de CTI por parte de los proveedores), las actividades manuales son aún las responsables de crear el núcleo de la producción en materia de CTI de las organizaciones.

- Las actividades de agregación de la información, análisis y difusión se gestionan principalmente utilizando **herramientas ampliamente disponibles** como las hojas de cálculo, correo y plataformas de gestión abiertas, lo que es indicativo de la eficiencia de las soluciones de bajo coste.

- La comunidad de usuarios de CTI entiende la importancia de definir los **requisitos de CTI**. Es la respuesta a las repetidas peticiones de los expertos en CTI[5.6] de reconocer la importancia de los requisitos de CTI y demuestra que esta comunidad ha seguido su consejo. También es interesante ver que un número importante de requisitos de CTI refleja las necesidades de las empresas y de los ejecutivos. Es una indicación de que la CTI está pasando a formar parte de la toma de decisiones en el ámbito de la gestión y de las empresas.
- El método más generalizado para crear **una base de conocimiento interna de CTI** es la combinación de consumo y producción. La tendencia principal es el aumento en la producción de CTI propia en las organizaciones, especialmente en el caso de la inteligencia derivada de sus propios análisis de datos brutos y alertas de amenazas contextualizadas. El consumo de información de fuentes de dominio público también se está convirtiendo en tendencia, considerando el aumento del uso de CTI disponible (canales de CTI de uso público como se indica en el punto siguiente).
- La **obtención de información a partir de fuentes de dominio público** es el método de consumo más utilizado, seguido por los canales de amenazas de proveedores de CTI. Es una tendencia en claro ascenso en 2020, que indica que los usuarios de CTI están invirtiendo en sus propias capacidades para producir inteligencia que se ajusta a sus necesidades.
- La **detección de amenazas** se evalúa como el caso de uso principal de la CTI. Aunque los indicadores del compromiso siguen siendo los elementos más importantes de la CTI para la detección de amenazas y para la respuesta a estas, el comportamiento de las amenazas y las tácticas del adversario (TTP) parecen ser las responsables del aumento en la tendencia en el uso de CTI en las organizaciones.
- Medir la **eficacia de la CTI** sigue siendo una tarea difícil, y solo un pequeño porcentaje de usuarios de CTI (4 %) implementan procesos para medir este parámetro. Se argumenta que, aunque las herramientas pueden añadir valor al análisis de la CTI, las capacidades de los analistas son el factor más importante para implementar con éxito la CTI. Un hallazgo interesante en lo que respecta al nivel de satisfacción es la baja puntuación que se da al valor de las funciones de aprendizaje automático.

Sinopsis

_Conclusiones y pasos siguientes

Considerando todos estos desarrollos en el ámbito de la CTI, se pueden extraer las siguientes conclusiones. A partir de estas conclusiones se indican los pasos siguientes, al menos desde el punto de vista de la ENISA, donde se va a reforzar la CTI de conformidad con su nuevo mandato, pero también teniendo en cuenta los desarrollos observados en las comunidades de las partes interesadas, como los Estados miembros, la Comisión Europea y otros organismos europeos, proveedores y usuarios finales de CTI:

- Dado el aumento en el número de partes interesadas de la UE y de los Estados miembros, la **cooperación y la coordinación de las actividades de la UE en materia de CTI** es clave. Además de reducir los costes de la CTI, la creación de sinergias también aumenta la confianza entre los agentes de la CTI y, por lo tanto, permite el uso compartido de inteligencia y de buenas prácticas en este campo. La ENISA promoverá la cooperación con varias de las partes interesadas al iniciar la **identificación de los requisitos de CTI.** Esto incluirá varios grupos de partes interesadas del ecosistema de organizaciones de la UE (como la Comisión, los organismos de la UE, agencias y Estados miembros).
- Como la relevancia de la CTI para las decisiones estratégicas y políticas está ampliamente aceptada, es importante **facilitar su conexión a la información geopolítica y a los sistemas físicos cibernéticos**. Esto permitirá incluir la CTI en los procesos de toma de decisiones de toda la UE y también permitirá la expansión de su contexto para identificar amenazas híbridas.

- **La integración de la CTI con los procesos de gestión de la seguridad** ayudará a que la inteligencia sobre las ciberamenazas prolifere en áreas relacionadas y contribuirá a identificar, detectar y prevenir las amenazas de forma oportuna. Uno de los efectos inmediatos será el aumento de la agilidad de procesos bastante prolongados (como las certificaciones o la evaluación de riesgos). Al mismo tiempo, la CTI facilitará la toma de decisiones de emergencia (p. ej., gestión de crisis) al proporcionar pruebas de exposición a ciberamenazas.
- Para responder mejor al aumento de las funciones de la CTI, la ENISA trabajará para **construir un programa de CTI exhaustivo**. El programa de CTI de la ENISA agrupará capacidades internas de forma horizontal para involucrar a todas las partes interesadas relacionadas en todas las fases de producción y difusión de CTI, y para desarrollar una infraestructura de CTI que se usará tanto de forma interna como para fines de formación.
- La inversión en algunos conceptos básicos de CTI, particularmente los relacionados con la **madurez y las jerarquías de la amenaza**, se considera muy útil para el aumento en la adopción de esta disciplina. La ENISA –junto con sus socios de la UE– dedicará su esfuerzo para desarrollar un modelo de madurez de la CTI. Asimismo, la ENISA consolidará y difundirá material de CTI multiuso útil, como jerarquías de amenaza que se pueden usar en otras áreas (p. ej., certificaciones, gestión de riesgos, panoramas sectoriales, etc.).

Algunas de las conclusiones y próximos pasos citados anteriormente serán la materia de trabajo de la ENISA en el campo de la CTI durante los próximos años.[35]

Bibliografía

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". 12 de marzo de 2020. EC-Council 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 de septiembre de 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". 20 de marzo de 2019. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. "2020 SANS Cyber Threat Intelligence (CTI) Survey". 10 de febrero de 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 de septiembre de 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 de octubre de 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

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

11. "Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts". Marzo de 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 de enero de 2020. Recorded Future. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

13. "A List of the Best Open Source Threat Intelligence Feeds". 4 de marzo de 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 de marzo de 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 de diciembre de 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-Council. 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" enero de 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". 19 de septiembre de 2019. CSIAC. https://www.csiac.org/journal-article/applying-cyber-threat-intelligence-to-industrial-control-systems/

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

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

34. "ENISA Programming Document", noviembre de 2019. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

35. «Reglamento sobre la Ciberseguridad de la UE» 7 de junio de 2019. Diario Oficial de la Unión Europea https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=ES

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

Lecturas relacionadas

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Revisión anual**

Un resumen de las tendencias en materia de ciberseguridad durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

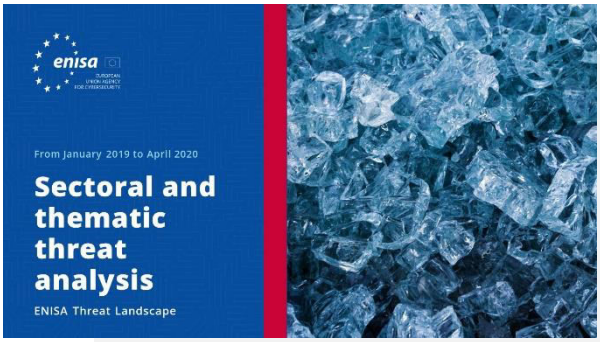
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Temas de investigación**

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia sobre las ciberamenazas.



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Incidentes principales en la UE y en el resto del mundo**

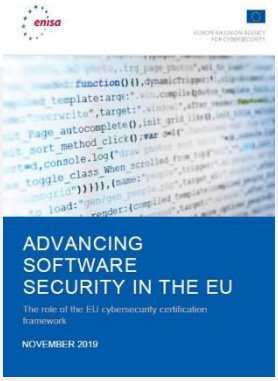
Incidentes de ciberseguridad principales que se han producido entre enero de 2019 y abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

Otras publicaciones



Avances en la seguridad de los programas informáticos en la UE

Presenta elementos clave de seguridad del software y ofrece un resumen conciso de los planteamientos más relevantes existentes y de los estándares en el panorama del desarrollo de programas informáticos seguros.

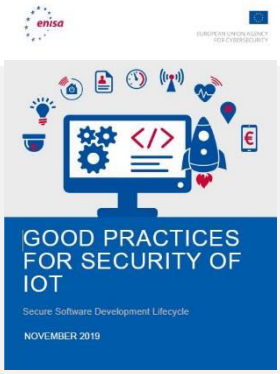
LEER EL INFORME

ENISA: Buenas prácticas para la seguridad de los vehículos inteligentes

Buenas prácticas para la seguridad de los vehículos inteligentes, vehículos conectados y semiautónomos para mejorar la experiencia del usuario y mejorar la seguridad del vehículo.

.

LEER EL INFORME



Buenas prácticas en la seguridad del IdC: ciclo de desarrollo de software seguro

Seguridad en el IdC con un enfoque especial a las directrices de desarrollo de programas informáticos.

LEER EL INFORME

«La relevancia de la CTI para las decisiones estratégicas y políticas está ampliamente aceptada y se considera esencial para facilitar la conexión a información geopolítica y a sistemas físicos cibernéticos»

en PAE 2020

¿Quiénes somos?

La agencia

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. La agencia se estableció en 2004, se ha visto reforzada por el Reglamento sobre la Ciberseguridad y contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC con programas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. A través del intercambio de conocimientos, la capacitación y la sensibilización, la Agencia coopera con las partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Puede encontrarse más información sobre la ENISA y su labor en www.enisa.europa.eu.

Colaboradores

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) y *todos los miembros del grupo de partes interesadas de CTI de la ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) y Thomas Hemker.

Editores

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

Datos de contacto

Las consultas acerca de este informe deben realizarse a través de enisa.threat.information@enisa.europa.eu.

Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic aquí.

Aviso legal

Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. Esta publicación tampoco refleja necesariamente la información más actual y ENISA se reserva el derecho a actualizarla en todo momento.

Las correspondientes fuentes de terceros se citan cuando proceda. ENISA declina toda responsabilidad por el contenido de las fuentes externas, incluidos los sitios *web* externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Además, debe poder accederse a la misma de forma gratuita. Ni ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

Aviso de copyright
© Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2020 Reproducción autorizada siempre que se indique la fuente.

Copyright de la imagen de la portada: © Wedia. Para utilizar o reproducir fotografías o cualquier otro material de cuyos derechos de autor no sea titular la ENISA, debe obtenerse el permiso directamente de los titulares de los derechos de autor.

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

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Reservados todos los derechos. Copyright ENISA 2020.

https://www.enisa.europa.eu