enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

Ianuarie 2019 – aprilie 2020

Prezentare generală a informațiilor privind amenințările cibernetice

Raportul ENISA privind situația amenințărilor

Prezentare generală

Evoluții în domeniul CTI

În acest raport, **evaluăm situația curentă a informațiilor privind amenințările cibernetice (CTI) ca domeniu dinamic de securitate cibernetică**. Această analiză își propune să indice principalele tendințe în dezvoltarea rapidă a CTI, oferind referințe relevante și rezumând pașii următori necesari pentru promovarea acestui subiect în anii următori.

În ianuarie 2020, ENISA a organizat un eveniment de consolidare a legăturilor comunității, **CTI-EU**. În cadrul acestui eveniment, diferite prezentări au demonstrat stadiul actual al CTI la nivel comercial, instituțional și de utilizator. Prezentările, discuțiile și demonstrațiile furnizorilor CTI au vizat starea produselor, abordărilor și practicilor și au indicat problemele existente. Este evident că **CTI a atins o maturitate suficientă și o masă critică** de materiale legate de CTI este acum disponibilă, de exemplu prin practici, instrumente și procese curente.

Se pare că **următoarea provocare din CTI va fi să absoarbă, să consolideze și să disemineze practicile existente** pentru a realiza o utilizare mai extinsă într-un mod sinergetic și eficient din punct de vedere al costurilor. Principalele oportunități în acest sens constau în schimbul de practici, cerințe, instrumente și informații CTI necompetitive. În afară de aceasta, identificarea noilor părți interesate care intră în activitatea CTI – atât producători, cât și consumatori – va spori capacitățile, va identifica cerințele standard CTI și va stabili capacitățile de partajare CTI în timp util. Atât prin evenimentul său CTI-UE, cât și prin cooperarea cu diferite părți interesate din UE, ENISA intenționează să consolideze sinergiile și să disemineze bunele practici CTI.

_Instrumente, materiale și practici CTI

Programul-cadru de cercetare Orizont 2020 al Comisiei_ Au fost finalizate diverse proiecte Orizont 2020 legate de CTI sau sunt încă în desfășurare. Acestea au cheltuit deja fonduri semnificative și au livrat o varietate de instrumente și practici pentru producerea, consumul și utilizarea CTI.

Practicile organismelor de standardizare, ale organizațiilor internaționale, ale guvernelor, ale industriei, ale mediului academic și ale utilizatorilor individuali_ Au fost dezvoltate o varietate de bune practici care acoperă: metode, cadre și modele de proces CTI[1,2,3] probleme de maturitate, cerințe, studii de utilizare, evaluarea instrumentelor[8,9,10], abordări pentru dezvoltarea CTI[11,12] etc.

Oferte CTI tip sursă deschisă_ Diverse fluxuri tip sursă deschisă[13] și instrumente care susțin OpenCTI[14] sunt importante pentru producători și consumatori, permițând accesul gratuit la CTI valoroase la un cost redus.

Instrumente (și practici) CTI tip sursă deschisă_ Au fost publicate numeroase instrumente, practici și articole tip sursă deschisă[15,16], care oferă abordări practice ale analizei și diseminării CTI utilizând instrumente tip sursă deschisă.[17,18,19]

Prezentare generală

_Oportunități de formare CTI

CYBRARY_ Introducere în domeniul informațiilor privind amenințările cibernetice.[21]

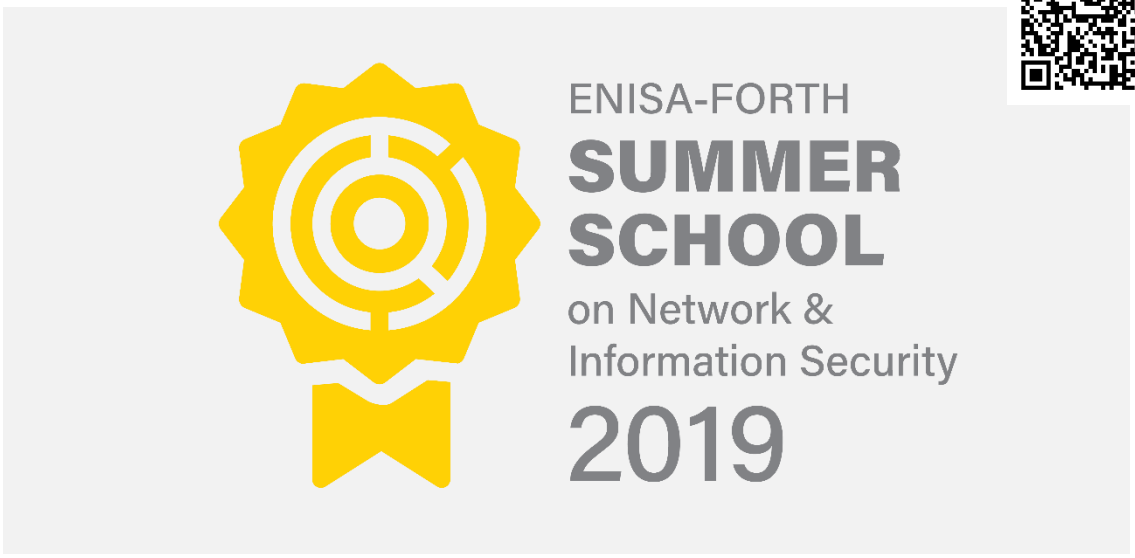
INSIKT_ Aflați mai multe despre „Protocoalele de certificare a informațiilor privind amenințările cibernetice”.[22]

SANS_ FOR578: Informații privind amenințările cibernetice.[23]

FIRST.org_ Simpozionul CTI.[24]

Gov.uk_Cyber_ Formare în domeniul informațiilor privind amenințările cibernetice (CRTIA).[25]

ENISA-FORTH_ Școala de vară NIS (Securitatea rețelelor și a informațiilor) – Formare în domeniul informațiilor privind amenințările cibernetice.[26]



ENISA-FORTH Școala de vară 2019

CTI-EU – Eveniment comunitar 2020

Prezentare generală

Lacune în materialele și practicile CTI disponibile

În pofida nivelurilor mai ridicate de maturitate atinse în ceea ce privește practicile și instrumentele CTI și furnizarea și consumul de CTI, există încă lacune în CTI, în special în ceea ce privește, printre altele, diferite cazuri de utilizare, CTI sectoriale și tipuri de CTI (operaționale, tactice, strategice). O astfel de lacună semnificativă a fost identificată în discuțiile din cadrul forumului ENISA CTI cu privire la disponibilitatea **CTI actualizate din atacuri** asupra sectoarelor și serviciilor critice. S-a convenit că elementele CTI (de exemplu, instrumente, tehnici și proceduri sau TTP-uri) incluse în diferite bune practici și cadre internaționale (de exemplu, ATT&CK[28]) trebuie să evolueze pentru a include informații dintr-un spectru mai larg de atacuri. Extrem de presante sunt elementele CTI ale diferitelor sectoare și infrastructuri și oferte de furnizare de servicii. Un exemplu în acest sens este lipsa de importanță acordată **atacurilor asupra cloud-computing.**[29] Pot apărea cereri similare din partea unor infrastructuri care sunt fie emergente (de exemplu, 5G[30]), fie de natură specializată, dar joacă un rol esențial în sistemele industriale critice, de exemplu, sistemele de control industrial (ICS) și sistemele de control de supraveghere și achiziție de date (SCADA).[31]

Deși cadrele existente pot conține diverse elemente utilizate în TTP-uri care vizează astfel de sisteme, aplicabilitatea lor în diferite sectoare va trebui extinsă pentru a ține seama de particularitățile TTP-urilor, cum ar fi abuzul interfețelor pentru programare de aplicații disponibile (application programming interfaces – API) și exploatarea activelor principale. În afară de TTP, elementele care vor necesita o analiză suplimentară sunt îndrumările privind **practicile de prevenire, detectare și atenuare** pentru aceste sectoare.

Aceasta va facilita dezvoltarea capacităților necesare și va permite utilizarea CTI concepute special pentru aceste sectoare. Principalul obstacol în calea diseminării CTI care pot da naștere la o acțiune pentru diferite tipuri de platforme și infrastructuri este intervalul dintre un incident, producerea CTI conexe și diseminarea acestor informații în instrumente de tip sursă deschisă. **O mai strânsă coordonare și cooperare** între părțile implicate va reduce timpul înainte ca CTI să fie puse la dispoziția comunității mai largi de utilizatori. Consolidarea încrederii între entitățile participante este cheia accelerării lanțului de aprovizionare CTI. Identificarea actorilor relevanți și mobilizarea comunității CTI sunt importante pentru a facilita aceste interacțiuni.

Un alt obstacol în calea dezvoltării capacităților necesare este disponibilitatea și consumul de CTI în cadrul diferitelor activități de gestionare a securității cibernetice. Exemplele includ gestionarea crizelor de securitate cibernetică, gestionarea incidentelor, răspunsul la incidente, vânarea amenințărilor și gestionarea vulnerabilităților. Această deficiență a fost evaluată în Raportul anterior al ENISA privind situația amenințărilor (ETL)[32] prin cicluri asincrone între disciplinele de securitate cibernetică și continuă să persiste.

În încheierea acestei secțiuni, trebuie remarcat faptul că deficiențele descrise nu se datorează lipsei de cunoștințe CTI în sine, ci mai degrabă ciclurilor lungi de comunicare și coordonare intrasectoriale și intersectoriale pentru schimbul de cunoștințe CTI.

Prezentare generală

_Probleme rezultate din construirea unei infrastructuri CTI

CTI sunt oferite în unele categorii largi în funcție de cerințele utilizatorilor pentru CTI, și anume operaționale, tactice și strategice. Ofertele comerciale existente constând în instrumente pentru colectarea, întreținerea, analiza și diseminarea CTI, fluxuri CTI, platforme cu informații privind amenințările (threat intelligence platform – TIP) etc. susțin unele dintre aceste tipuri de CTI. Cu toate acestea, nu există o abordare unică.

Ofertele existente se concentrează pe CTI operaționale și tactice, în timp ce CTI strategice sunt oferite de cele mai multe ori independent.

Cu toate acestea, limitele dintre CTI sunt destul de neclare. Urmare a acestui fapt, atunci când un consumator CTI dorește să-și construiască o capacitate și mediul corespunzător pentru a gestiona CTI, selectarea elementelor adecvate nu este simplă. Aceasta se datorează în principal faptului că **furnizarea de servicii CTI și peisajul instrumentelor CTI existente sunt oarecum fragmentate**. Pentru a încerca să construiască un astfel de mediu, utilizatorii de CTI vor trebui să selecteze cel mai bun sistem din ofertele existente. Selecția trebuie să îndeplinească cerințele CTI, precum și practicile și procesele în materie de CTI aplicate, ținând cont de obiectivele lor curente și viitoare de maturitate a CTI.

Deși au fost elaborate anumite criterii/cerințe pentru selectarea TIP-urilor[33] pentru diferite profiluri de utilizatori de CTI, vor fi necesare cerințe similare pentru alte produse, servicii și instrumente în materie de CTI. În mod ideal, astfel de cerințe se vor concentra pe diferite niveluri de maturitate a utilizatorilor, niveluri de cheltuieli și tipuri de CTI. Criterii/cerințe similare sunt necesare pentru alte elemente ale unei infrastructuri CTI, cum ar fi instrumente, bune practici, platforme de partajare etc.

Pe termen lung, OpenCTI[14] poate fi o soluție bună pentru abordarea problemelor cauzate de fragmentarea ofertelor CTI, având în vedere capacitatea sa inerentă de a integra surse CTI de diferite tipuri într-un singur mediu de prelucrare.

În anul următor, părțile interesate ale ENISA și CTI vor depune eforturi pentru evaluarea cerințelor de infrastructură CTI și verificarea modului în care acestea pot fi îndeplinite de produsele CTI existente. Aceste acțiuni vor demara cu încercarea de a stabili o infrastructură CTI pentru nevoile interne ale ENISA în vederea dezvoltării unei platforme CTI pentru CTI strategice.

Prezentare generală

Valorificarea CTI în disciplinele conexe securității cibernetice

Încorporarea CTI în disciplinele cheie ale securității cibernetice a fost deja identificată ca o problemă de către membrii comunității CTI. Este în special cazul activităților și componentelor de gestionare a securității care sunt legate de medii extrem de dinamice, cu expunere sporită, cum ar fi dispozitivele utilizatorului (de exemplu, USIMS, token-uri de securitate, dispozitive mobile, sisteme industriale, dispozitive de e-sănătate etc.). Alte discipline conexe care pot beneficia în mod semnificativ de CTI sunt activitățile de certificare, practicile de gestionare a crizelor, criminalistica computerizată și răspunsul la incidente, printre altele.

ENISA recunoaște[35] necesitatea **includerii CTI în domeniul certificării**. În 2020, ENISA a înființat un grup de lucru ad-hoc cu scopul de a integra gestionarea riscurilor și CTI cu practicile de identificare a nivelurilor de asigurare.

În special, CSA afirmă că ***„Nivelul de asigurare trebuie să fie proporțional cu nivelul riscului asociat utilizării intenționate a produsului TIC, a serviciului TIC sau a procesului TIC, în ceea ce privește probabilitatea și impactul unui incident"*** **[articolul 52 alineatul (1)].**

Astfel, este evident faptul că CTI trebuie să fie incluse în procesul de certificare utilizând o evaluare a nivelului de asigurare. Deși părți ale CTI sunt prevăzute în standardele de certificare[36] prin utilizarea unui „profil de atacator", acest concept cuprinde o mică parte din CTI disponibile.

Activitatea desfășurată de **grupul de lucru ad-hoc al ENISA** constă în combinarea informațiilor din evaluările riscurilor și amenințărilor (CTI) pentru a grupa în mod corespunzător cerințele de protecție și pentru a le corela cu diferite niveluri de asigurare. Corelarea se va baza pe diferite niveluri de risc care rezultă din expunerea activelor la amenințare și, în același timp, dau naștere la propuneri privind numărul și amploarea controalelor de atenuare. Aceste controale vor determina selectarea funcțiilor de securitate care vor fi atribuite mai multor niveluri de asigurare și vor fi supuse implementării de diferitele obiective de certificare (ToC).

Activitățile ENISA cu privire la acest subiect se desfășoară cu sprijinul unui grup de experți, care combină abilitățile de gestionare a riscurilor, CTI și certificare. Activitățile au început în aprilie 2020 și vor fi finalizate în al treilea trimestru al anului 2020. Rezultatele acestei activități vor fi publicate de ENISA.

Prezentare generală

_Rezultatele unui sondaj CTI cuprinzător

Dintr-un sondaj CTI reprezentativ[7], se pot extrage numeroase concluzii interesante cu privire la nivelul actual de adoptare a practicilor și instrumentelor CTI. Printre altele, sondajul reflectă stadiul actual al capacităților CTI, tipurile de CTI utilizate în rândul părților interesate, interacțiunea practicilor CTI cu alte procese din organizații și cazurile de utilizare a instrumentelor CTI.

În această discuție, rezultatele sondajului sunt extrapolate la experiențele acumulate de ENISA în cadrul propriilor activități (strategice) CTI și la răspunsurile primite din partea unor părți interesate CTI diferite în cadrul forumurilor CTI UE și europene[36]. În acest context, accentul este plasat pe identificarea cerințelor, culegerea de informații, producerea de CTI strategice, utilizarea instrumentelor și practicilor și integrarea cu alte procese relevante. În acest sens, am dori să subliniem următoarele puncte.

- Una dintre concluziile principale din acest raport este că **semiautomatizarea producției de CTI** este un instrument important: în timp ce automatizarea absorbției de informații este în creștere – în pofida unei creșteri a consumului de CTI de către furnizori – activitățile manuale continuă să alcătuiască nucleul producției de CTI a organizațiilor.

- Activitățile de agregare, analiză și diseminare a informațiilor sunt gestionate utilizând **instrumente disponibile pe scară largă**, cum ar fi foi de calcul, corespondență și platforme de gestionare de tip sursă deschisă, ceea ce indică eficiența soluțiilor cu costuri reduse.

- Importanța definirii **cerințelor CTI** este înțeleasă de comunitatea de utilizatori CTI. Aceasta vine ca răspuns la pledoariile repetate ale experților CTI[5,6] despre recunoașterea semnificației cerințelor CTI și arată că comunitatea CTI a urmat recomandările acestora. De asemenea, este interesant de văzut că un număr semnificativ de cerințe CTI reflectă nevoile întreprinderilor și ale directorilor. Acesta este un indiciu că CTI devine parte a procesului decizional la nivel de întreprinderi și de conducere.
- O combinație de consum și producție de CTI este metoda predominantă pentru construirea unei **baze de cunoștințe CTI** interne. Tendința principală este creșterea producției proprii de CTI în cadrul organizațiilor, în special pentru CTI derivate din propria lor analiză a datelor brute și a alertelor de amenințare contextualizate. Consumul din surse disponibile publicului devine o tendință, având în vedere utilizarea crescândă a CTI disponibile (fluxuri CTI de tip sursă deschisă, astfel cum este indicat la punctul de mai jos).
- **Culegerea informațiilor tip sursă deschisă** este cea mai utilizată metodă de absorbție, urmată de fluxurile de amenințări de la furnizorii de CTI. Aceasta este o tendință ascendentă clară în 2020, indicând faptul că utilizatorii CTI investesc în propriile capacități pentru a produce CTI care le respectă cerințele.
- **Detectarea amenințărilor** este evaluată ca principal caz de utilizare pentru CTI. Deși indicatorii de compromis (IoC) reprezintă în continuare cele mai importante elemente ale CTI în detectarea amenințărilor și răspunsul la amenințări, comportamentul amenințărilor și tactica adversă (TTP) par să fie responsabili pentru tendințele ascendente în utilizarea CTI în organizații.
- Măsurarea **eficacității CTI** este în continuare o sarcină dificilă și doar un procent mic de utilizatori CTI (4 %) aplică procese pentru a măsura eficiența CTI. Se susține că, deși instrumentele pot adăuga valoare în analiza CTI, abilitățile analistului sunt cele mai importante pentru aplicarea cu succes a CTI. O constatare interesantă cu privire la nivelul de satisfacție este calificativul scăzut acordat valorii funcțiilor de învățare automatizată.

Prezentare generală

Concluzii și etapele următoare

Având în vedere toate aceste evoluții în domeniul CTI, se pot formula următoarele concluzii. Pe baza acestor concluzii sunt indicați o serie de pași de urmat, cel puțin din punctul de vedere al ENISA, în cazul căreia CTI vor fi consolidate în conformitate cu noul său mandat, dar luând în considerare și evoluțiile observate în comunitățile sale de părți interesate precum statele membre, Comisia Europeană și alte organisme europene, furnizorii și utilizatorii finali de CTI:

- Având în vedere numărul tot mai mare de părți interesate din UE și statele membre, **cooperarea și coordonarea activităților CTI la nivelul UE** sunt esențiale. În timp ce construirea pe baza sinergiilor poate reduce costurile CTI, aceasta sporește și încrederea în rândul actorilor CTI, permițând astfel schimbul de CTI și de bune practici. ENISA va promova cooperarea cu diferiți actori prin inițierea **identificării cerințelor CTI.** Aceasta va include mai multe grupuri de părți interesate din cadrul ecosistemului de organizații UE (și anume, Comisia, organismele UE, agențiile și statele membre).
- Pe măsură ce se înțelege relevanța CTI pentru luarea de decizii strategice și politice, este important **să se faciliteze legătura sa cu informațiile geopolitice și sistemele cibernetice**. Acest lucru va permite includerea CTI în procesele decizionale, dar va facilita și extinderea contextului său la amenințările hibride identificate.

- **Integrarea CTI cu procesele de gestionare a securității** va ajuta CTI să prolifereze în domenii conexe și va contribui la identificarea, detectarea și prevenirea amenințărilor în timp util. Un efect imediat va fi creșterea agilității proceselor destul de durabile (de exemplu, certificarea, evaluarea riscurilor). În același timp, CTI va facilita luarea deciziilor de urgență (de exemplu, gestionarea crizelor), oferind dovezi privind expunerea la amenințări cibernetice.
- Pentru a răspunde mai bine la rolul crescând al CTI, ENISA va lucra la **consolidarea unui program cuprinzător de CTI**. Programul CTI al ENISA va include competențe interne pe orizontală pentru a înscrie toate părțile interesate conexe în toate fazele producției și diseminării CTI și va dezvolta o infrastructură CTI care va fi utilizată atât în scopuri interne, cât și de formare.
- Investițiile în unele concepte CTI de bază, în special **maturitatea CTI și ierarhiile amenințărilor**, sunt considerate foarte utile pentru creșterea gradului de utilizare a CTI. ENISA – împreună cu partenerii săi din UE – va investi unele eforturi în dezvoltarea unui model de maturitate a CTI. Mai mult, ENISA consolidează și diseminează materiale multifuncționale utile privind CTI, cum ar fi ierarhii ale amenințărilor care pot fi utilizate în alte domenii (de exemplu, certificarea, gestionarea riscurilor, peisajele sectoriale etc.).

Unele dintre concluziile de mai sus și pașii următori vor face obiectul activității ENISA în domeniul CTI în anii următori.[35]

Referințe

1. „CyberThreat Intelligence Lab” (Laborator de informații privind amenințările cibernetice). HPI și TU Delft. https://www.cyber-threat-intelligence.com/

2. „5-Step process to power your Cyber Defense with Cyber Threat Intelligence” (Proces în 5 etape pentru a vă alimenta apărarea cibernetică cu informații privind amenințările cibernetice) 12 martie 2020. Blogul Consiliului CE. https://blog.eccouncil.org/5-step-process-to-power-your-cyber-defense-with-cyber-threat-intelligence/

3. „The Cycle of Cyber Threat Intelligence” (Ciclul informațiilor privind amenințările cibernetice) 3 septembrie 2019. SANS, https://www.youtube.com/watch?v=J7e74QLVxCk

4 „Maturing Cyber Threat Intelligence” (Maturarea informațiilor privind amenințările cibernetice) HPI și TU Delft. https://www.cyber-threat-intelligence.com/maturity/

5. „Intelligence Requirements: the Sancho Panza of CTI” (Cerințe de informații: Sancho Panza al CTI). Andreas Sfakianakis. https://threatintel.eu/2019/09/24/intelligence-requirements-and-don-quixote/

6. „Your requirements are not my requirements” (Cerințele dvs. nu sunt cerințele mele). 20 martie 2019. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. „2020 SANS Cyber Threat Intelligence (CTI) Survey” [Sondaj SANS 2020 al informațiilor privind amenințările cibernetice (CTI)] 10 februarie 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” (Lista celor mai importante instrumente CTI pentru hackeri și profesioniști din domeniul securității). 9 septembrie 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” (Ce sunt informațiile privind amenințările cibernetice? Definiție și tipuri) 25 octombrie 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

10. „The Ultimate Guide to Cyber Threat Intelligence (CTI) in 2020” (Ghidul definitiv privind CTI în 2020). 15 iunie 2020. AI Multiple. https://research.aimultiple.com/cti/

11. „Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts” (Informațiile privind amenințările cibernetice în guvern: un ghid pentru factorii de decizie și analiști). Martie 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” (Ce înseamnă cele 6 faze ale ciclului de viață a informațiilor privind amenințările cibernetice pentru echipa dvs.). 15 ianuarie 2020. Recorded Future. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

13. „A List of the Best Open Source Threat Intelligence Feeds” (Lista celor mai bune fluxuri de informații de sursă deschisă privind amenințările cibernetice). 4 martie 2020. Logz.io. https://logz.io/blog/open-source-threat-intelligence-feeds/

14. „Open Cyber Threat Intelligence Platform” (Platforma deschisă de informații privind amenințările cibernetice). OpenCTI. https://www.opencti.io/en/

15. „The Cyber Intelligence Analyst Cookbook Volume 1” (Ghidul analistului informațiilor cibernetice, volumul 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” [Informații din surse deschise (OSINT): exemplu practic]. 16 martie 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" (De ce facem parte din CONCORDIA – cel mai mare consorțiu european de securitate cibernetică). 11 decembrie 2019. Ericson. https://www.ericsson.com/en/blog/2019/12/concordia-telco-threat-intelligence-platform

19. „1st Newsletter of CYBER-TRUST project" (Primul buletin informativ al proiectului CYBER-TRUST) Aditess. https://aditess.com/main/2020/01/30/1st-newsletter-of-cyber-trust-project/

20. CTIA Exam Blueprint v1 (Planul examenului CTIA v1). Consiliul CE. https://www.eccouncil.org/wp-content/uploads/2019/04/CTIA-Exam-Blueprint-v1.pdf

21. Intro to Cyber Threat Intelligence (Introducere în informațiile privind amenințările cibernetice). Cybrary. https://www.cybrary.it/course/intro-cyber-threat-intelligence/

22. Learning More about The Cyber Threat Intelligence Certification Protocols (Aflați mai multe despre protocoalele de certificare a informațiilor privind amenințările cibernetice). INSIKT. https://www.insiktintelligence.com/cyber-threat-intelligence-certification/

23. Cyber Threat Intelligence Summit (Summit-ul privind informațiile privind amenințările cibernetice). SANS. https://www.sans.org/event/cyber-threat-intelligence-summit-2020

24. FIRST Cyber Threat Intelligence Symposium (Simpozion-ul FIRST privind informațiile privind amenințările cibernetice). FIRST. https://www.first.org/events/symposium/zurich2020/program

25. Cyber Threat Intelligence Training (CRTIA) [Formare în domeniul informațiilor privind amenințările cibernetice (CRTIA)]. Gov.uk. https://www.digitalmarketplace.service.gov.uk/g-cloud/services/599285779458382

26. NIS Summer School – CTI Training (Școala de vară NIS – Formare CTI). 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" (Dilema contextului CTI Cloud), ianuarie 2020. NetScope. https://www.enisa.europa.eu/events/2019-cti-eu/presentations/the-cti-cloud-context-dilema

30. „ENISA Threat Landscape for 5G Networks" (Raportul ENISA privind situația amenințărilor pentru rețelele 5G) Octombrie 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

31. „Applying Cyber Threat Intelligence to Industrial Control System" (Aplicarea CTI la sistemul de control industrial). 19 septembrie 2019. CSIAC. https://www.csiac.org/journal-article/applying-cyber-threat-intelligence-to-industrial-control-systems/

32. „ENISA Threat Landscape Report 2018" (Raportul ENISA privind situația amenințărilor în 2018) Martie 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

33. „Exploring the opportunities and limitations of current Threat Intelligence Platforms" (Explorarea oportunităților și a limitărilor platformelor actuale de informații despre amenințări). 26 martie 2018. ENISA. https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

34. „ENISA Programming Document" (Document de programare ENISA). Noiembrie 2019. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

35. „EU Cybersecurity Act" (Regulamentul UE privind securitatea cibernetică). 7 iunie 2019. Jurnalul Oficial al Uniunii Europene. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019R0881&from=EN

36. „CTI-EU | Bonding EU Cyberthreat Intelligence" (Crearea de legături între informațiile privind amenințările cibernetice UE)https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence

Documente conexe

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Trecerea în revistă a anului**

Un rezumat al tendințelor de securitate cibernetică pentru perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

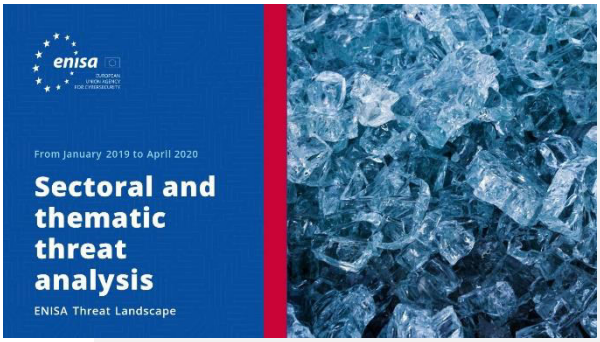
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare din diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.



CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Analiza sectorială și tematică a amenințărilor**

Analiza contextualizată a amenințărilor în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Incidente principale în UE și în întreaga lume**

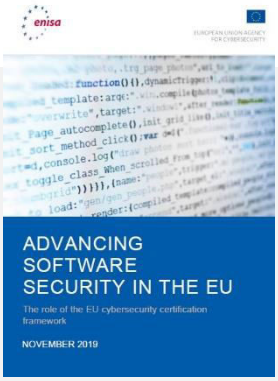
Principalele incidente de securitate cibernetică survenite în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

Alte publicații



Promovarea securității software-ului în UE

Prezintă elemente cheie ale securității software-ului și oferă o imagine de ansamblu concisă asupra celor mai relevante abordări și standarde existente în peisajul dezvoltării de software-uri sigure.

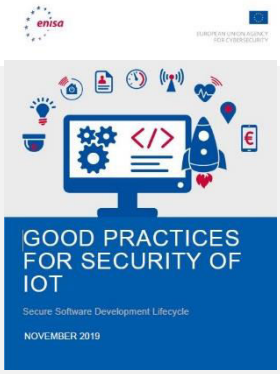
CITIȚI RAPORTUL

Bune practici ENISA pentru securitatea mașinilor inteligente

Bune practici pentru securitatea mașinilor inteligente, și anume vehiculele conectate și (semi)autonome, pentru a spori experiența utilizatorilor de mașini și pentru a îmbunătăți siguranța mașinii

.

CITIȚI RAPORTUL



Bune practici pentru securitatea internetului obiectelor (Internet of Things – IoT) – Ciclul de viață al dezvoltării software-ului sigur

Securitatea internetului obiectelor (Internet of Things – IoT), cu un accent special pe orientările în materie de dezvoltare de software.

CITIȚI RAPORTUL

„Pe măsură ce este înțeleasă relevanța CTI pentru luarea deciziilor strategice și politice, este important să se faciliteze legătura sa cu informațiile geopolitice și sistemele cibernetice”

în ETL 2020

Despr
e

Agenție

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică
contribuie la politica cibernetică a UE, sporește credibilitatea produselor, serviciilor și proceselor TIC cu ajutorul sistemelor de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa sunt disponibile la adresa www.enisa.europa.eu.

Contribuitori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) și *toți membrii Grupului părților interesate al ENISA CTI:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) și Thomas Hemker.

Editori

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

Date de contact

Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

Dorim să aflăm părerea dumneavoastră despre acest raport!
Vă rugăm să acordați câteva momente completării chestionarului. Pentru a accesa formularul, faceți clic aici.

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

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu