enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Omówienie kwestii rozpoznawania cyberzagrożeń

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

_Postępy w dziedzinie CTI

W tym raporcie **oceniamy aktualny stan wiedzy o rozpoznawaniu cyberzagrożeń (cyber threat intelligence, CTI) jako dynamicznej domeny bezpieczeństwa cybernetycznego**. Niniejsze opracowanie ma na celu wskazanie głównych trendów w szybkim rozwoju CTI poprzez przedstawienie odpowiednich odniesień i podsumowanie kolejnych kroków, niezbędnych do rozwinięcia tego tematu w nadchodzących latach.

W styczniu 2020 r. ENISA zorganizowała integrujące środowisko sympozjum **CTI-EU**. Przedstawione podczas tego wydarzenia prezentacje ukazały aktualny stan CTI na poziomach komercyjnym, instytucjonalnym i użytkownika. Prezentacje, dyskusje i demonstracje dostawców CTI dotyczyły stanu produktów, podejść i praktyk oraz wskazywały istniejące problemy. Widać wyraźnie, że **CTI osiągnęło wystarczającą dojrzałość, a masa krytyczna** materiałów związanych z CTI jest już dostępna, np. poprzez aktualne praktyki, narzędzia i procesy.

Wydaje się, że **następnym wyzwaniem w zakresie CTI będzie przejrzenie, konsolidacja i rozpowszechnianie istniejących praktyk** dla osiągnięcia szerszego zastosowania w ekonomiczny i synergiczny sposób. Główne możliwości w tym zakresie to współdzielenie niekonkurencyjnych praktyk, wymagań, narzędzi i informacji CTI. Ponadto rozpoznanie nowych zainteresowanych stron rozpoczynających działalność CTI – zarówno producentów, jak i konsumentów – zwiększy możliwości, określi standardowe wymagania CTI i ustanowi możliwości współdzielenia CTI w odpowiednim czasie. Poprzez sympozjum CTI-EU oraz współpracę z zainteresowanymi stronami z UE, ENISA planuje wzmocnić synergie i rozpowszechniać dobre praktyki CTI.

_Narzędzia, materiały i praktyki CTI

Badania i koncepcje ramowe programu „Horyzont 2020" Komisji_ Różne projekty H2020 związane z CTI zostały już ukończone lub wciąż są w toku. Pochłonęły już znaczne fundusze i dostarczyły różnorodnych narzędzi i praktyk tworzenia, konsumpcji i wykorzystania CTI.

Praktyki organów normalizacyjnych, organizacji międzynarodowych, rządów, przemysłu, środowisk akademickich i użytkowników indywidualnych_ Opracowano szereg dobrych praktyk, obejmujących: Metody, koncepcje ramowe i modele procesów CTI[1,2,3]; kwestie dojrzałości, wymagania, badania wykorzystania, ocenę narzędzi[8,9,10]; podejścia do opracowywania CTI[11,12] itd.

Oferty CTI open source_ Różne kanały open source[13] i narzędzia zgodne z OpenCTI[14] są ważne dla producentów i konsumentów, umożliwiając im bezpłatny dostęp do wartościowego CTI przy niskich kosztach.

Narzędzia (i praktyki) CTI open source_ Udostępniono wiele narzędzi, praktyk i artykułów open source[15,16], które dostarczają praktycznych podejść do analizy i rozpowszechniania CTI przy użyciu narzędzi typu open source[17,18,19].

Informacje ogólne

_Możliwości szkoleń w zakresie CTI

CYBRARY_ Wprowadzenie do analizy zagrożeń cybernetycznych[21].

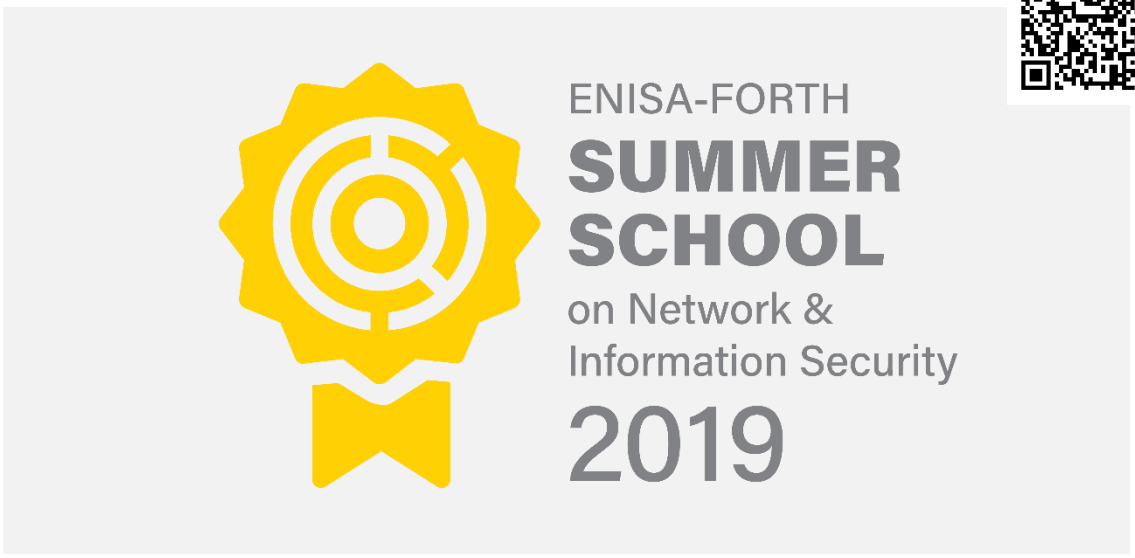
INSIKT_ „Learning More about The Cyber Threat Intelligence Certification Protocols”[22].

SANS_ FOR578: Analiza zagrożeń cybernetycznych[23].

FIRST.org_ Cyber Threat Intelligence Symposium[24].

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

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



Letnia szkoła ENISA-FORTH 2019

Wydarzenie społecznościowe CTI-EU 2020

Informacje ogólne

Luki w dostępnych materiałach i praktykach CTI

Mimo wzrostu poziomu dojrzałości praktyk i narzędzi CTI oraz dostarczania i korzystania z CTI, w CTI wciąż istnieją luki, w szczególności w odniesieniu do różnych przypadków użycia, sektorowych CTI i rodzajów CTI (operacyjnego, taktycznego, strategicznego). Taką istotną lukę wskazano w dyskusji na forum ENISA CTI na temat dostępności **aktualnych CTI pochodzących z ataków** na sektory i usługi krytyczne. Uzgodniono, że elementy CTI (np. narzędzia, techniki i procedury – TTP) zawarte w różnych międzynarodowych dobrych praktykach i koncepcjach ramowych (np. ATT i CK[28]) muszą ewoluować, aby uwzględnić analizy szerszego spektrum ataków. Szczególnie palącą potrzebą są elementy CTI dla różnych sektorów oraz infrastruktur i ofert dostawców usług. Przykładem tego jest brak nacisku na ataki na **przetwarzanie w chmurze**[29]. Podobne żądania mogą dotyczyć infrastruktury, która albo dopiero powstaje (np. 5G[30]), albo ma charakter specjalistyczny, ale odgrywa kluczową rolę w krytycznych systemach przemysłowych, na przykład automatyki przemysłowej (ICS) czy nadzorowania procesów technologicznych (SCADA)[31].

Chociaż istniejące koncepcje ramowe mogą zawierać różne elementy wykorzystywane w TTP ukierunkowanych na takie systemy, ich zastosowanie w różnych sektorach będzie musiało zostać zwiększone, aby uwzględnić szczególne cechy TTP, takie jak nadużywanie dostępnych interfejsów programowania aplikacji (API) i wykorzystanie podstawowych zasobów Oprócz TTP elementami, które będą wymagały dalszego rozważenia, są wytyczne dotyczące **praktyk zapobiegania, wykrywania i łagodzenia skutków** dla tych sektorów.

Ułatwi to rozwój niezbędnych zdolności i umożliwi korzystanie z CTI tworzonych specjalnie dla tych sektorów. Główną przeszkodą w upowszechnianiu odpowiednich CTI dla różnych rodzajów platform i infrastruktury jest upływ czasu między incydentem, wytworzeniem powiązanego CTI i wprowadzeniem tych informacji do narzędzi open source. **Ściślejsza koordynacja i współpraca** między zaangażowanymi stronami skróci czas potrzebny do udostępniania CTI szerszemu gronu użytkowników. Budowanie zaufania wśród uczestniczących podmiotów ma kluczowe znaczenie dla przyspieszenia łańcucha dostaw CTI. Dla ułatwienia tych interakcji ważne są określenie uczestników i mobilizacja społeczności CTI.

Kolejną przeszkodą w budowaniu niezbędnych zdolności jest dostępność i wykorzystanie CTI w ramach różnych działań związanych z zarządzaniem bezpieczeństwem cybernetycznym. Przykłady obejmują zarządzanie w sytuacjach kryzysowych związanych z bezpieczeństwem cybernetycznym, zapobieganie i ograniczanie skutków incydentów, reagowanie na incydenty, wykrywanie zagrożeń i eliminowanie podatności. Niedociągnięcie to, które nadal się utrzymuje, oceniono w poprzednim raporcie o krajobrazie zagrożeń, ENISA Threat Landscape (ETL)[32], jako brak synchronizacji cykli między dyscyplinami cyberbezpieczeństwa.

Podsumowując tę sekcję, należy zauważyć, że opisane niedociągnięcia nie wynikają z braku wiedzy o CTI jako takiej, ale raczej z długich cykli komunikacji międzysektorowej i wewnątrzsektorowej oraz koordynacji wymiany wiedzy CTI.

Informacje ogólne

_Problemy wynikające z budowy infrastruktury CTI

CTI dzieli się na kilka szerokich kategorii zgodnych z wymaganiami użytkowników – operacyjne, taktyczne i strategiczne. Istniejące oferty komercyjne, obejmujące narzędzia do gromadzenia, utrzymywania, analizy i rozpowszechniania CTI, kanałów CTI, platform analizy zagrożeń (TIP) itp. wspierają niektóre z tych rodzajów CTI. Nie ma wszakże jednego uniwersalnego podejścia.

Istniejące oferty koncentrują się na operacyjnym i taktycznym CTI, zaś strategiczne CTI jest głównie oferowane niezależnie.

Jednak granice między poszczególnymi rodzajami CTI są raczej rozmyte. W efekcie, gdy użytkownik CTI chce zbudować możliwości i odpowiednie środowisko zarządzania CTI, wybór odpowiednich elementów nie jest prosty. Dzieje się tak głównie dlatego, że **świadczenie usług CTI i oferta istniejących narzędzi CTI są w pewnym stopniu rozdrobnione**. Budując takie środowisko, użytkownicy CTI będą musieli wybrać system najlepszy w swojej klasie spośród istniejących ofert. Wybór ten musi odpowiadać wymaganiom CTI oraz zastosowanym praktykom i procesom CTI, przy uwzględnieniu obecnych i przyszłych celów dotyczących dojrzałości CTI.

Choć zostały opracowane pewne kryteria/wymagania dotyczące wyboru TIP[33] dla różnych profili użytkowników CTI, podobne wymagania będą konieczne dla dalszych produktów, usług i narzędzi CTI. Idealnie byłoby, gdyby takie wymagania skupiały się na różnych poziomach dojrzałości użytkowników, poziomach wydatków i rodzajach CTI. Podobne kryteria/wymagania są też niezbędne dla innych elementów infrastruktury CTI, takich jak narzędzia, dobre praktyki, platformy udostępniania itp.

W dłuższej perspektywie dobrym rozwiązaniem problemów spowodowanych fragmentacją ofert może być CTI OpenCTI[14] ze względu na jego zdolność do integracji różnych źródeł CTI w jednym środowisku narzędziowym.

W nadchodzącym roku ENISA i podmioty zaangażowane w CTI będą pracować nad oceną wymagań dotyczących infrastruktury CTI oraz tego, jak mogą one zostać spełnione przez istniejące produkty CTI. Działania te rozpocznie próba utworzenia infrastruktury CTI na potrzeby wewnętrzne ENISA w celu opracowania platformy CTI dla strategicznych CTI.

Informacje ogólne

Wykorzystanie CTI w powiązanych dyscyplinach bezpieczeństwa cybernetycznego

Włączenie CTI do kluczowych dyscyplin bezpieczeństwa cybernetycznego zostało już wskazane jako problem przez członków społeczności CTI. Dotyczy to w szczególności działań i komponentów zarządzania bezpieczeństwem, które są związane z wysoce dynamicznymi środowiskami o zwiększonej ekspozycji, takimi jak urządzenia użytkownika (np. USIMS, tokeny zabezpieczające, urządzenia mobilne, systemy przemysłowe, urządzenia medyczne itp.). Inne powiązane dyscypliny, które mogą znacząco skorzystać na CTI, to między innymi działalność certyfikacyjna, praktyki zarządzania kryzysowego, cyber-kryminalistyka i reagowanie na incydenty.

ENISA uznaje[35] potrzebę **włączenia CTI do obszaru certyfikacji**. W roku 2020 ENISA powołała doraźną grupę roboczą, której celem jest zintegrowanie zarządzania ryzykiem i CTI z praktykami określania poziomów pewności.

W szczególności CSA stanowi, że ***„poziom pewności powinien być współmierny do poziomu ryzyka związanego z planowanym wykorzystaniem produktu ICT, usługi ICT lub procesu ICT, pod względem prawdopodobieństwa i skutków incydentu"*** **(art. 52(1)).**

W związku z tym jest oczywiste, że CTI musi wejść w proces certyfikacji przez ocenę poziomu pewności. Choć elementy CTI są przewidziane w standardach certyfikacji[36] przez użycie „profilu atakującego", koncepcja ta obejmuje niewielką część dostępnych CTI.

Praca **doraźnej grupy roboczej ENISA** polega na łączeniu informacji pochodzących z ocen ryzyka i zagrożeń (CTI) w celu odpowiedniego grupowania wymogów w zakresie ochrony i przypisania ich do różnych poziomów pewności. Przypisanie będzie oparte na różnych poziomach ryzyka, które wynikają z ekspozycji zasobów na zagrożenie, a jednocześnie będzie stanowić podstawę propozycji dotyczących liczby i siły środków zaradczych. Środki te będą determinować wybór funkcji bezpieczeństwa, które zostaną przypisane do wielu poziomów pewności i będą podlegały wdrożeniu przez różne cele certyfikacji (ToC).

Prace ENISA w tym zakresie prowadzone są przy wsparciu grupy ekspertów z dziedziny zarządzania ryzykiem, CTI i certyfikacji. Rozpoczęły się w kwietniu 2020 r., a zakończą się w III kwartale 2020 r. Wyniki tych prac zostaną opublikowane przez ENISA.

Informacje ogólne

_Wyniki kompleksowej ankiety CTI

Z reprezentatywnej ankiety CTI[7] można wyciągnąć wiele interesujących wniosków na temat aktualnego wykorzystania praktyk i narzędzi CTI. Badanie odzwierciedla między innymi aktualny stan możliwości CTI, rodzaje CTI stosowane przez ankietowanych, wzajemne oddziaływanie praktyk CTI z innymi procesami w organizacjach oraz przypadki użycia narzędzi CTI.

W tej dyskusji wyniki ankiety są ekstrapolowane do doświadczeń zdobytych przez ENISA w ramach jej własnych (strategicznych) działań CTI oraz informacji zwrotnych od różnych zainteresowanych stron CTI na unijnych i europejskich forach CTI[36]. W tym kontekście nacisk kładziony jest na określenie wymagań, zbieranie informacji, tworzenie strategicznych CTI, stosowanie narzędzi i praktyk oraz integrację z innymi istotnymi procesami. W związku z tym chcielibyśmy zwrócić uwagę na poniższe kwestie.

- Jednym z głównych wniosków płynących z raportu jest to, że **półautomatyzacja tworzenia CTI** jest ważnym narzędziem: podczas gdy automatyzacja pozyskiwania informacji rośnie – mimo wzrostu wykorzystania CTI przez dostawców – czynności ręczne nadal stanowią rdzeń tworzenia CTI w organizacji.

- Działania związane z agregowaniem, analizą i rozpowszechnianiem informacji są wykonywane za pomocą **szeroko dostępnych narzędzi**, takich jak arkusze kalkulacyjne, poczta i platformy zarządzania typu open source, co świadczy o efektywności tanich rozwiązań.

- Społeczność użytkowników CTI rozumie istotność zdefiniowania **wymagań CTI**. Jest to odpowiedź na powtarzające się apele ekspertów CTI[5,6] o uznanie znaczenia wymagań CTI i pokazuje, że społeczność CTI skorzystała z ich rad. Ciekawe jest również to, że znaczna część wymagań CTI odzwierciedla potrzeby biznesu i kadry kierowniczej. Oznacza to, że CTI staje się częścią procesu podejmowania decyzji na poziomie firmy i kierownictwa.
- Dominującą metodą budowania wewnętrznej **bazy wiedzy CTI** jest połączenie wykorzystania i tworzenia CTI. Głównym trendem jest wzrost samodzielnego tworzenia CTI przez organizacje, zwłaszcza w przypadku CTI wynikającego z własnej analizy danych pierwotnych i kontekstowych alertów o zagrożeniach. Trendem staje się korzystanie z publicznie dostępnych źródeł, biorąc pod uwagę rosnące użycie dostępnych CTI (źródła CTI typu open source, jak wskazano w punkcie poniżej).
- Najczęściej stosowaną metodą pozyskiwania informacji jest **zbieranie informacji open source**, a zaraz po niej pojawiają się informacje o zagrożeniach od dostawców CTI. Jest to trend wyraźnie rosnący w 2020 r., co wskazuje, że użytkownicy CTI inwestują we własne możliwości tworzenia CTI zgodnego z ich wymaganiami.
- Jako główny przypadek użycia CTI oceniane jest **wykrywanie zagrożeń**. Choć nadal najważniejszymi elementami CTI w wykrywaniu zagrożeń i reagowaniu na nie są wskaźniki zagrożenia (IoC), za wzrostowe trendy stosowania CTI w organizacjach wydają się być odpowiedzialne zachowania związane z zagrożeniami i taktyki przeciwnika (TTP).
- Pomiar **efektywności CTI** jest wciąż trudnym zadaniem i tylko niewielki odsetek użytkowników CTI (4%) wdraża procesy pomiaru efektywności CTI. Argumentuje się, że choć w analizie CTI narzędzia mogą stanowić wartość dodaną, najważniejsze dla pomyślnego wdrożenia CTI są umiejętności analityka. Ciekawym spostrzeżeniem w obszarze poziomu satysfakcji jest niska ocena wartości funkcji uczenia maszynowego.

Informacje ogólne

Wnioski i kolejne kroki

Biorąc pod uwagę wszystkie postępy w dziedzinie CTI, można wyciągnąć podane poniżej wnioski. Na podstawie tych wniosków wskazano kolejne kroki, przynajmniej z punktu widzenia ENISA, w ramach których CTI ma zostać wzmocnione zgodnie z jego nowym mandatem, ale z uwzględnieniem zmian obserwowanych w społecznościach zainteresowanych stron, takich jak państwa członkowskie, Komisja Europejska i inne europejskie organy, dostawcy i użytkownicy końcowi CTI:

- Biorąc pod uwagę rosnącą liczbę zainteresowanych stron w UE i państwach członkowskich, **współpraca i koordynacja ogólnounijnych działań CTI** ma kluczowe znaczenie. Budowanie na synergii może obniżyć koszty CTI, a jednocześnie zwiększa zaufanie między podmiotamiama CTI, umożliwiając w ten sposób dzielenie się CTI i dobrymi praktykami. ENISA będzie promować współpracę z różnymi zainteresowanymi stronami, inicjując **określanie wymagań CTI.** Obejmie to wiele grup zainteresowanych stron w ekosystemie organizacji UE (tj. Komisja oraz organy, agencje i państwa członkowskie UE).
- Ponieważ znaczenie CTI dla podejmowania decyzji strategicznych i politycznych jest zrozumiałe, ważne, aby **ułatwić jego połączenie z informacjami geopolitycznymi i systemami cybernetyczno-fizycznymi**. Umożliwi to włączenie CTI do procesów decyzyjnych, a także pozwoli na rozszerzenie jego kontekstu o identyfikację zagrożeń hybrydowych.

- **Integracja CTI z procesami zarządzania bezpieczeństwem** pomoże upowszechniać CTI w powiązanych obszarach i przyczyni się do szybkiej identyfikacji, wykrywania i zapobiegania zagrożeniom. Bezpośrednim efektem będzie zwiększenie sprawności dość długotrwałych procesów (np. certyfikacji, oceny ryzyka). Jednocześnie CTI ułatwi podejmowanie decyzji w sytuacjach wyjątkowych (np. zarządzanie kryzysowe), dostarczając dowodów na ekspozycję na zagrożenia cybernetyczne.
- Aby lepiej reagować na rosnącą rolę CTI, ENISA będzie pracować nad **stworzeniem kompleksowego programu CTI**. Program ENISA CTI połączy poziomo umiejętności wewnętrzne, by zaangażować wszystkich powiązanych interesariuszy na wszystkich etapach tworzenia i rozpowszechniania CTI oraz opracować infrastrukturę CTI, która będzie wykorzystywana zarówno do celów wewnętrznych, jak i szkoleniowych.
- Inwestowanie w niektóre podstawowe koncepcje CTI, w szczególności **dojrzałość CTI i hierarchie zagrożeń**, uważa się za bardzo sprzyjające zwiększaniu upowszechnienia CTI. ENISA – wraz ze swoimi partnerami z UE – dołoży starań, aby opracować model dojrzałości CTI. Ponadto ENISA będzie konsolidować i rozpowszechniać przydatne, wielofunkcyjne materiały CTI, takie jak hierarchie zagrożeń, które można wykorzystać w innych obszarach (np. certyfikacja, zarządzanie ryzykiem, krajobrazy sektorowe itp.).

Niektóre z powyższych wniosków i kolejnych kroków będą przedmiotem prac ENISA w obszarze CTI w najbliższych latach[35].

Bibliografia

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

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

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

4. „Maturing Cyber Threat Intelligence". HPI i 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 marca 2019 r. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. „2020 SANS Cyber Threat Intelligence (CTI) Survey". 10 lutego 2020 r. 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 września 2019 r. 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 października 2019 r. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

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

11. „Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts". Marzec 2019 r. 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 stycznia 2020 r. Recorded Future. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

13. „A List of the Best Open Source Threat Intelligence Feeds". 4 marca 2020 r. 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 marca 2020 r. 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 grudnia 2019 r. Ericsson. 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" Styczeń 2020 r. NetScope. https://www.enisa.europa.eu/events/2019-cti-eu/presentations/the-cti-cloud-context-dilema

30. „ENISA Threat Landscape for 5G Networks" Październik 2019 r. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

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

32. „Raport ENISA o krajobrazie zagrożeń 2018" (ENISA Threat Landscape Report) marzec 2019 r. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

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

34. „ENISA Programming Document" Listopad 2019 r. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

35. „Akt o cyberbezpieczeństwie" 7 czerwca 2019 r. Dziennik Urzędowy Unii Europejskiej. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

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

Powiązany

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Przegląd roku

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

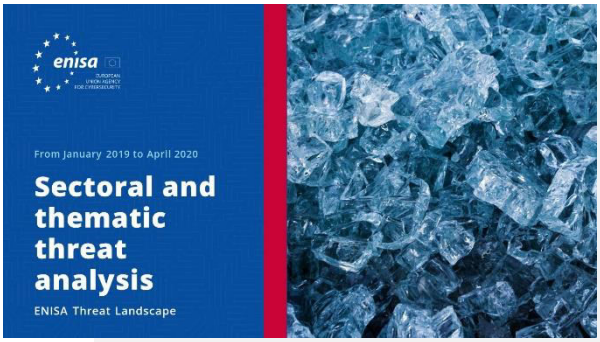
Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie bezpieczeństwa cybernetycznego i analizy zagrożeń cybernetycznych.



Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Najważniejsze incydenty w UE i na świecie

Najważniejsze incydenty związane z cyberbezpieczeństwem w okresie od stycznia 2019 r. do kwietnia 2020 r.

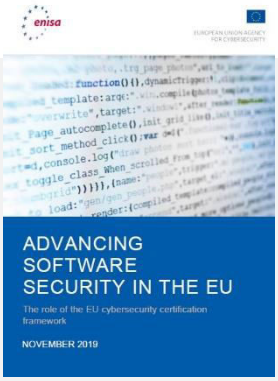
PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Inne publikacje



Zwiększanie bezpieczeństwa oprogramowania w UE

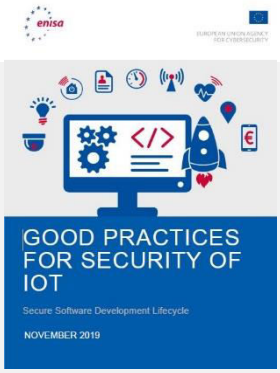
Przedstawia kluczowe elementy bezpieczeństwa oprogramowania i oferuje zwięzły przegląd najistotniejszych dotychczasowych metod i standardów w sferze bezpiecznego rozwoju oprogramowania.

PRZECZYTAJ RAPORT

Dobre praktyki ENISA dotyczące bezpieczeństwa inteligentnych samochodów

Dobre praktyki dotyczące bezpieczeństwa inteligentnych samochodów, a mianowicie połączonych i (pół)autonomicznych pojazdów, mające na celu poprawę wrażeń użytkowników i bezpieczeństwa samochodów
.

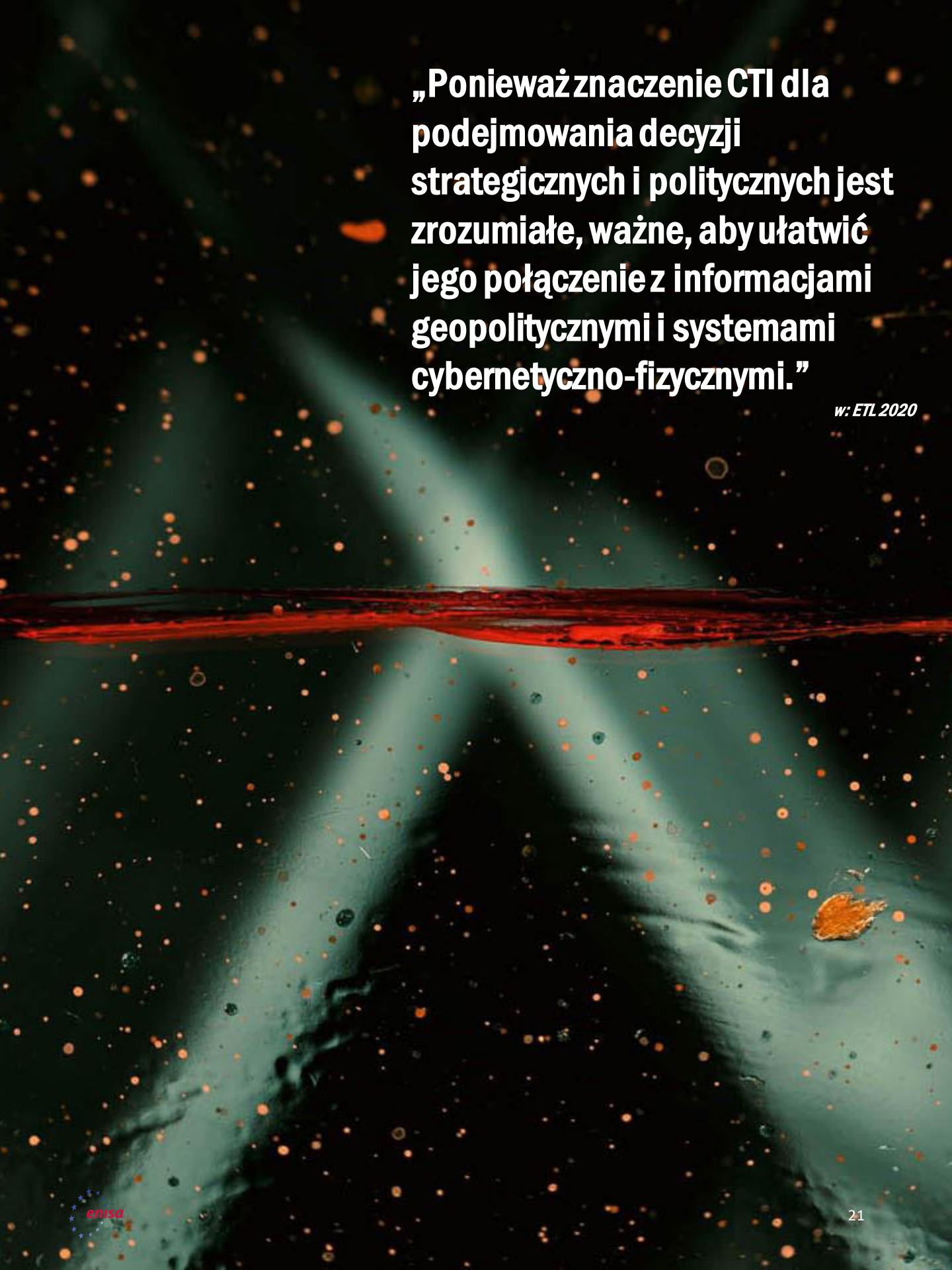
PRZECZYTAJ RAPORT



Dobre praktyki dotyczące bezpieczeństwa IoT – cykl życia tworzenia bezpiecznego oprogramowania

Bezpieczeństwo ioT ze szczególnym uwzględnieniem wytycznych dotyczących tworzenia oprogramowania.

PRZECZYTAJ RAPORT



„Ponieważ znaczenie CTI dla podejmowania decyzji strategicznych i politycznych jest zrozumiałe, ważne, aby ułatwić jego połączenie z informacjami geopolitycznymi i systemami cybernetyczno-fizycznymi."

w: ETL 2020

Informacje o age

Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; podnosi wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Przez wymianę informacji, budowanie zdolności i zwiększanie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do połączonej gospodarki i odporność unijnej infrastruktury oraz, ostatecznie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

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

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

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

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu