IT

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Da gennaio 2019 ad aprile 2020

Quadro generale dell'intelligence sulle minacce informatiche

Panorama delle minacce

Quadro generale

_Sviluppi nell'area della CTI

In questa relazione **valutiamo la situazione attuale dell'intelligence sulle minacce informatiche (Cyber Threat Intelligence, CTI) come dominio dinamico della cibersicurezza**. L'analisi è finalizzata a indicare le principali tendenze delineatesi nel rapido sviluppo della CTI, fornendo riferimenti pertinenti e riepilogando i passi successivi da intraprendere per promuovere questo argomento negli anni a venire.

Nel gennaio 2020 l'ENISA ha organizzato un proprio evento di connessione della community di **CTI a livello UE**[2], in occasione del quale varie presentazioni hanno illustrato la situazione attuale della CTI a livello commerciale, istituzionale e di utenti. Presentazioni, discussioni e dimostrazioni di fornitori di servizi di CTI hanno affrontato lo stato dei prodotti, gli approcci e le pratiche e hanno indicato i problemi esistenti. È evidente che la **CTI ha raggiunto un livello di maturità sufficiente e che una massa critica** di materiale sull'argomento è ormai disponibile, ad esempio attraverso le pratiche, gli strumenti e i processi attuali.

Sembra che la **prossima sfida nella CTI sarà quella di elaborare, consolidare e diffondere le pratiche esistenti** per arrivare a un utilizzo più ampio, in modo efficiente in termini di costi e sinergico. Le principali opportunità a questo riguardo risiedono nella condivisione di pratiche non competitive, requisiti, strumenti e informazioni in materia di CTI. Oltre a questo, l'individuazione di nuovi portatori di interessi che entrano nell'attività della CTI, sia produttori sia consumatori, migliorerà le funzionalità, identificherà i requisiti standard e stabilirà le capacità di condivisione in tema di CTI in modo tempestivo. Grazie all'evento CTI-UE così come alla cooperazione con i vari portatori di interessi dell'UE, l'ENISA intende rafforzare le sinergie e diffondere le buone pratiche in materia di CTI.

_Strumenti, materiali e pratiche di CTI

Programma quadro di ricerca e innovazione Orizzonte 2020 della Commissione_ Vari progetti di Orizzonte 2020 legati alla CTI sono stati completati o sono in corso. Hanno già utilizzato fondi significativi e fornito una varietà di strumenti e pratiche per la produzione, la fruizione e l'utilizzo della CTI.

Pratiche di enti di normalizzazione, organizzazioni internazionali, pubbliche amministrazione, industria, università e singoli utenti_ Sono state messe a punto svariate buone pratiche che riguardano: metodi, quadri di riferimento e modelli di processo di CTI[1,2,3] problemi di maturità, requisiti, indagini sull'uso, valutazione degli strumenti[8,9,10], approcci allo sviluppo della CTI[11,12], ecc.

Offerte di CTI open source_ Vari feed[13] e strumenti open source che supportano OpenCTI[14] sono importanti per produttori e consumatori, consentendo il libero accesso a una preziosa CTI a costi contenuti.

Strumenti (e pratiche) di CTI open source_ Sono stati pubblicati numerosi strumenti, pratiche e articoli open source[15,16] che forniscono approcci pratici all'analisi e alla diffusione della CTI attraverso strumenti da fonte aperta[17,18,19]

Quadro generale

_Opportunità di formazione sulla CTI

CYBRARY_ Introduction to Cyber Threat Intelligence.[21]

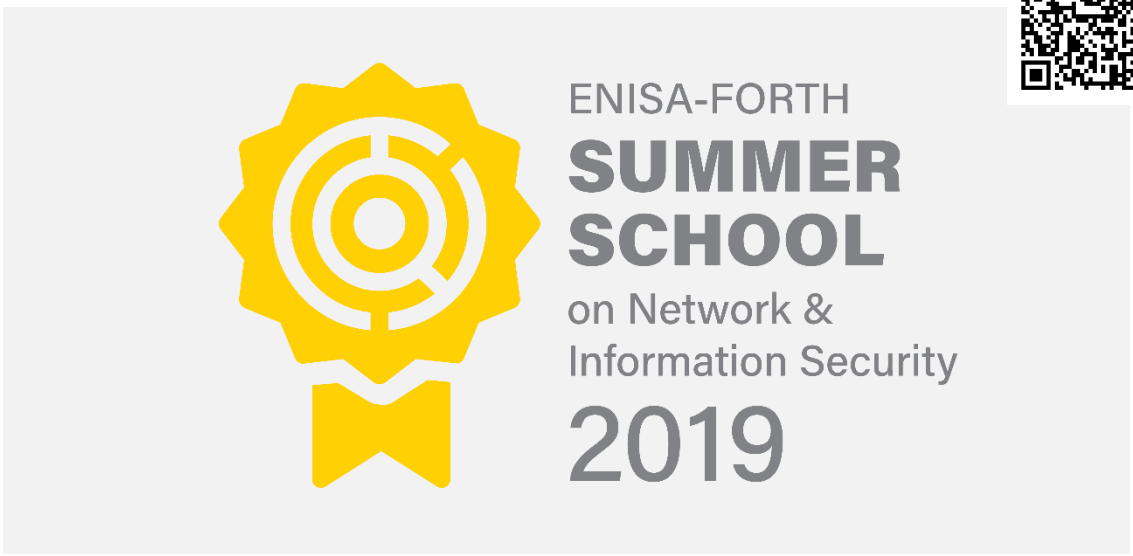
INSIKT_ Learning more about the «Cyber Threat Intelligence Certification Protocols».[22]

SANS_ FOR578: Cyber Threat Intelligence.[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]



ENISA-FORTH Summer School 2019

CTI-EU Community Event 2020

Quadro generale

_Le lacune nei materiali e nelle pratiche di CTI disponibili

A dispetto dei più alti livelli di maturità raggiunti nelle pratiche e negli strumenti di CTI, e nelle relative fornitura e fruizione, permangono lacune in particolare per quanto riguarda, tra l'altro, i vari casi d'uso, la CTI settoriale e le tipologie di CTI (operativa, tattica, strategica). Una lacuna significativa è stata individuata nella discussione all'interno del forum CTI dell'ENISA in merito alla disponibilità di **CTI aggiornata derivata dagli attacchi** a settori e servizi critici. Si è convenuto sulla necessità di un'evoluzione degli elementi della CTI (ad esempio tattiche, tecniche e procedure o TTP) inclusi in varie buone pratiche e quadri di riferimento internazionali (quali ATT&CK)[28]), al fine di includere l'intelligence derivata da un più ampio spettro di attacchi. Particolarmente urgenti sono gli elementi di CTI di vari settori e infrastrutture e offerte di fornitura di servizi. Ne è un esempio la mancanza di attenzione verso gli **attacchi al cloud computing**.[29] Richieste analoghe possono scaturire da infrastrutture emergenti (ad esempio il 5G[30]) o che sono di natura specialistica pur svolgendo un ruolo essenziale in sistemi industriali critici, ad esempio i sistemi di controllo industriale (ICS) e i sistemi di controllo di supervisione e acquisizione dati (SCADA).[31]

Sebbene i quadri di riferimento esistenti possano contenere vari elementi utilizzati nelle TTP destinate a tali sistemi, sarà necessario espanderne l'applicabilità in vari settori per tenere conto delle peculiarità delle TTP, come l'abuso delle interfacce di programmazione delle applicazioni (API) disponibili e lo sfruttamento degli asset principali. Oltre alle TTP, gli elementi che richiederanno un'ulteriore considerazione sono gli orientamenti in merito alle **pratiche di prevenzione, rilevamento e mitigazione** per questi settori.

Ciò faciliterà lo sviluppo delle capacità necessarie e consentirà l'uso di CTI specifica per questi settori. L'ostacolo principale alla diffusione di CTI utilizzabile per vari tipi di piattaforme e infrastrutture è il tempo che intercorre tra un incidente, la produzione della CTI correlata e l'inserimento di queste informazioni in strumenti open source. **Un coordinamento e una cooperazione più stretti** tra le parti coinvolte ridurranno il tempo necessario perché la CTI sia messa a disposizione della vasta comunità di utenti. Creare un clima di fiducia tra le entità partecipanti è essenziale per accelerare la catena di fornitura della CTI. Identificare gli attori rilevanti e mobilitare la comunità della CTI sono importanti per agevolare queste interazioni.

Un'altra barriera alla creazione delle capacità necessarie è costituita dalla disponibilità e dalla fruizione della CTI nell'ambito di varie attività di gestione della sicurezza informatica. Alcuni esempi sono la gestione delle crisi di cibersicurezza, la gestione degli incidenti, la risposta agli incidenti, la ricerca proattiva delle minacce («threat hunting») e la gestione delle vulnerabilità. Questa carenza è stata oggetto di valutazione nella precedente relazione sul Panorama delle minacce analizzato dall'ENISA (ETL)[32] mediante cicli asincroni tra le discipline della cibersicurezza e permane tuttora.

Per concludere la sezione, va notato che le carenze descritte non sono imputabili a una mancanza di conoscenza della CTI in sé, ma piuttosto ai lunghi cicli di comunicazione e coordinamento intersettoriali e intrasettoriali per lo scambio di tale conoscenza.

Quadro generale

_Problematiche emergenti dalla creazione di un'infrastruttura di CTI

La CTI viene offerta in alcune ampie categorie secondo le esigenze degli utenti in materia, ovvero come operativa, tattica e strategica. Le offerte commerciali esistenti, costituite da strumenti per la raccolta, la gestione, l'analisi e la diffusione di CTI, feed di CTI, piattaforme di intelligence sulle minacce (TIP), ecc. supportano alcune di queste tipologie di CTI. Non esiste tuttavia un approccio valido per tutti i casi.

Le offerte esistenti si concentrano sulla CTI operativa e tattica, mentre quella strategica viene per lo più proposta in modo indipendente.

I confini tra le varie tipologie sono comunque piuttosto confusi. Ne deriva che, quando un fruitore di CTI desidera creare una funzionalità e l'ambiente corrispondente per gestire la CTI, la selezione degli elementi adatti non è immediata. Questo soprattutto perché **la fornitura di servizi di CTI e il panorama degli strumenti esistenti sono piuttosto frammentati**. Per tentare di creare un tale ambiente, gli utenti di CTI dovranno selezionare un sistema «best of breed» tra le offerte esistenti. La scelta deve soddisfare i requisiti di CTI e le pratiche e i processi applicati, tenendo conto degli obiettivi attuali e futuri in termini di maturità della CTI.

Sebbene siano stati elaborati alcuni criteri e requisiti per la scelta di piattaforme TIP[33] per vari profili di utente, requisiti analoghi saranno necessari per ulteriori prodotti, servizi e strumenti di CTI. Idealmente, tali requisiti si concentreranno su vari livelli di maturità degli utenti, livelli di spesa e tipologie di CTI. Criteri e requisiti analoghi sono necessari per vari altri elementi di un'infrastruttura di CTI, come strumenti, buone pratiche, piattaforme di condivisione, ecc.

Nel lungo periodo OpenCTI[14] potrebbe essere una valida soluzione per affrontare i problemi causati dalla frammentazione delle offerte, data la sua capacità intrinseca di integrare fonti di CTI di vario tipo in un unico ambiente di strumenti.

Nel prossimo anno l'ENISA e i portatori di interessi si impegneranno a valutare i requisiti infrastrutturali della CTI e a verificare come essi possano essere soddisfatti con i prodotti di CTI esistenti. Si partirà dal tentativo di creare un'infrastruttura di CTI per le esigenze interne dell'ENISA, al fine di sviluppare una piattaforma per la CTI strategica.

Quadro generale

_Sfruttare la CTI nelle discipline di cibersicurezza correlate

Incorporare la CTI nelle discipline chiave della sicurezza informatica è già stato identificato come problema dalla community della CTI. Ciò vale in particolare per le attività di gestione della sicurezza e per le componenti legate ad ambienti altamente dinamici caratterizzati da una maggiore esposizione, come i dispositivi degli utenti (ad esempio USIM, token di sicurezza, dispositivi mobili, sistemi industriali, dispositivi di e-health, ecc.). Altre discipline correlate che possono trarre significativi benefici dalla CTI sono, tra le altre, attività di certificazione, pratiche di gestione delle crisi, informatica forense e risposta agli incidenti.

L'ENISA riconosce[35] la necessità di **includere la CTI nell'area della certificazione**. Nel 2020 l'ENISA ha istituito un gruppo di lavoro ad hoc con l'obiettivo di integrare la gestione del rischio e la CTI con le pratiche per l'identificazione dei livelli di affidabilità.

Nello specifico, il regolamento sulla cibersicurezza afferma che ***«[i]l livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente»*** **(articolo 52, paragrafo 1).**

Risulta perciò evidente che la CTI debba confluire nel processo di certificazione mediante una valutazione del livello di affidabilità. Sebbene parti della CTI siano previste nelle norme di certificazione[36] con l'utilizzo di un «profilo dell'aggressore», questo concetto comprende una piccola porzione della CTI disponibile.

Il compito del **gruppo di lavoro ad hoc dell'ENISA** consiste nel combinare in modo appropriato le informazioni provenienti dalle valutazioni dei rischi e delle minacce (CTI) con le esigenze di protezione del gruppo e nel mapparle a vari livelli di affidabilità. La mappatura si baserà sui vari livelli di rischio che emergono dall'esposizione degli asset alle minacce e, allo stesso tempo, darà origine a proposte in termini di numero e forza dei controlli di mitigazione. Tali controlli determineranno la scelta delle funzioni di sicurezza che saranno assegnate a più livelli di affidabilità e saranno soggetti ad attuazione da parte dei vari obiettivi di certificazione (Target of Certification, ToC).

Il lavoro dell'ENISA su questo tema si svolge con il sostegno di un gruppo di esperti, grazie a una combinazione di competenze di gestione del rischio, CTI e certificazione. Il lavoro è iniziato nell'aprile 2020 e si concluderà nel terzo trimestre del 2020. I risultati saranno pubblicati dall'ENISA.

Quadro generale

_Risultati di un'indagine esaustiva sulla CTI

Da un'indagine rappresentativa della CTI[7] è possibile trarre numerose conclusioni interessanti sull'attuale diffusione delle pratiche e degli strumenti in materia. L'indagine riflette, tra l'altro, la situazione corrente delle funzionalità della CTI, le tipologie di CTI utilizzate tra i portatori di interessi, l'interazione delle pratiche di CTI con altri processi nelle organizzazioni e i casi d'uso degli strumenti di CTI.

In questa trattazione i risultati dell'indagine vengono estrapolati alle esperienze acquisite dall'ENISA nell'ambito delle proprie attività di CTI (strategica) e al feedback dei vari portatori di interessi all'interno dell'UE e dei forum europei sulla CTI[36]. In questo contesto, l'attenzione è rivolta all'identificazione dei requisiti, alla raccolta di informazioni, alla produzione di CTI strategica, all'uso di strumenti e pratiche e all'integrazione con altri processi pertinenti. Desideriamo a tale riguardo evidenziare i punti seguenti.

- Una delle principali conclusioni di questa relazione è che la **semi-automazione della produzione di CTI** è uno strumento importante: anche se si osserva un incremento dell'automazione dell'ingestione di informazioni, malgrado l'aumento della fruizione di CTI da parte dei fornitori, le attività manuali costituiscono ancora il nucleo della produzione di CTI delle organizzazioni.
- Le attività di aggregazione, analisi e diffusione delle informazioni sono gestite mediante **strumenti ampiamente disponibili**, quali fogli di calcolo, posta e piattaforme di gestione open source, un dato indicativo dell'efficienza delle soluzioni a basso costo.

- L'importanza di definire **requisiti di CTI** è compresa dalla comunità di utenti. Questo è in risposta ai ripetuti appelli degli esperti[5,6] a riconoscere l'importanza dei requisiti di CTI e dimostra che la comunità di CTI ha seguito i loro consigli. È interessante anche notare che una parte significativa di requisiti di CTI rispecchia le esigenze delle imprese e dei dirigenti, a indicazione del fatto che la CTI sta entrando a far parte del processo decisionale a livello aziendale e manageriale.
- Una combinazione di fruizione e produzione di CTI è il metodo prevalente per costruire una **base di conoscenze sulla CTI** interna. L'incremento di CTI prodotta in proprio dalle organizzazioni è la tendenza principale, soprattutto per la CTI derivata dalla loro analisi dei dati grezzi e dagli avvisi di minacce contestualizzati. La fruizione da fonti pubblicamente disponibili sta diventando una tendenza, considerato il crescente utilizzo di CTI disponibile (feed di CTI open source, come indicato al punto seguente).
- La **raccolta di informazioni open source** è il metodo di ingestione più utilizzato, seguito dai feed delle minacce provenienti dai fornitori di CTI. Si rileva una chiara tendenza al rialzo nel 2020, a indicazione del fatto che gli utenti di CTI stanno investendo nelle proprie funzionalità per produrre CTI conforme ai loro requisiti.
- Il **rilevamento delle minacce** è valutato come il principale caso d'uso per la CTI. Sebbene gli indicatori di compromissione (Indicators of Compromise, IoC) restino gli elementi più importanti della CTI nel rilevamento, nella risposta e nel comportamento riguardo alle minacce così come nelle tattiche avversarie (TTP), essi sembrano essere responsabili del tendenziale aumento dell'uso della CTI nelle organizzazioni.
- Misurare l'**efficacia della CTI** si conferma un compito difficile e solo un'esigua percentuale di utenti (4%) attua processi per misurare l'efficienza della CTI. Si sostiene che, sebbene la strumentazione possa aggiungere valore all'analisi della CTI, le competenze dell'analista sono l'elemento più importante per la buona riuscita dell'implementazione della CTI. Un risultato interessante riguardo al livello di soddisfazione è la bassa valutazione assegnata al valore delle funzioni di apprendimento automatico.

Quadro generale

_Conclusioni e passi successivi

Considerati tutti questi sviluppi nell'ambito della CTI, è possibile trarre le seguenti conclusioni. Sulla base di queste conclusioni sono indicati alcuni passi successivi, quanto meno dal punto di vista dell'ENISA, dove la CTI sarà rafforzata in conformità al suo nuovo mandato, ma anche tenendo conto degli sviluppi osservati nelle sue comunità di portatori di interessi, come gli Stati membri, la Commissione europea e altri organismi europei, i fornitori e gli utenti finali della CTI:

- Dato il numero crescente di portatori di interessi a livello dell'UE e degli Stati membri, **la cooperazione e il coordinamento** sono essenziali. Se da un lato il rafforzamento delle sinergie può ridurre i costi della CTI, dall'altro esso incrementa anche la fiducia tra gli attori, consentendo così la condivisione della CTI e delle buone pratiche. L'ENISA promuoverà la cooperazione con vari portatori di interessi avviando l'**individuazione dei requisiti della CTI.** Saranno coinvolti diversi gruppi di portatori di interessi all'interno dell'ecosistema delle organizzazioni dell'UE (vale a dire la Commissione, gli organismi, le agenzie e gli Stati membri dell'Unione).
- Man mano che viene compresa la pertinenza della CTI per le decisioni strategiche e politiche, è importante **agevolarne il collegamento con le informazioni geopolitiche e i sistemi ciberfisici**. Ciò consentirà l'inclusione della CTI nei processi decisionali, permettendo inoltre di ampliarne il contesto all'identificazione delle minacce ibride.

- **L'integrazione della CTI con i processi di gestione della sicurezza** ne favorirà la diffusione nelle aree correlate e contribuirà all'individuazione tempestiva, al rilevamento e alla prevenzione delle minacce. Un effetto immediato sarà la maggiore agilità dei processi di durata relativamente lunga (quali certificazione, valutazione del rischio). Allo stesso tempo, la CTI faciliterà il processo decisionale in caso di emergenza (ad esempio la gestione delle crisi) fornendo prove in merito all'esposizione alle minacce informatiche.
- Per rispondere meglio al ruolo crescente della CTI, l'ENISA lavorerà alla **costruzione di un programma di CTI completo**, che riunirà orizzontalmente le competenze interne per coinvolgere tutti i portatori di interessi in tutte le fasi della produzione e della diffusione della CTI e che svilupperà un'infrastruttura CTI destinata sia a finalità interne sia di formazione.
- Gli investimenti in alcuni concetti di base, in particolare **maturità della CIT e gerarchia delle minacce**, sono ritenuti molto utili per accrescere la diffusione della CTI. L'ENISA, insieme ai suoi partner dell'UE, si impegnerà nello sviluppo di un modello di maturità della CTI; inoltre, consoliderà e diffonderà materiale utile e polivalente sulla CTI, come le gerarchie delle minacce utilizzabili in altre aree (ad esempio certificazione, gestione del rischio, scenari settoriali, ecc.).

Alcune delle conclusioni e dei passi successivi riportati in precedenza costituiranno l'oggetto del lavoro dell'ENISA nell'ambito della CTI nel corso dei prossimi anni.[35]

Riferimenti bibliografici

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 marzo 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 settembre 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 marzo 2019. Pasquale Stirparo. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

7. «2020 SANS Cyber Threat Intelligence (CTI) Survey». 10 febbraio 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 settembre 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 ottobre 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

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

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

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

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

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

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

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

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

35. «Regolamento UE sulla cibersicurezza» 7 giugno 2019. Gazzetta ufficiale dell'Unione europea. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=IT

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

Correlati

Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Elenco delle prime 15 minacce**

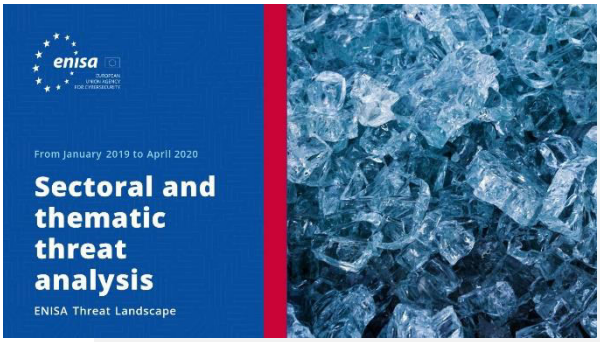
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Argomenti di ricerca**

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.

LEGGI LA RELAZIONE



Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Incidenti principali nell'UE e a livello mondiale**

Principali incidenti di cibersicurezza verificatisi tra gennaio 2019 e aprile 2020.

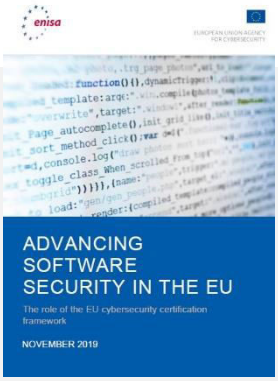
LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Altre pubblicazioni



Advancing Software Security in the EU (Promuovere la sicurezza del software nell'UE)

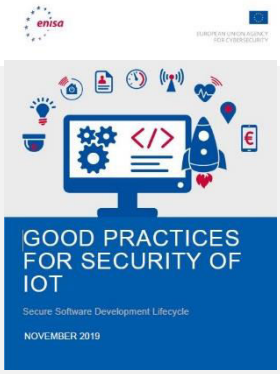
Presenta gli elementi chiave della sicurezza del software e fornisce un quadro conciso degli approcci e degli standard esistenti più pertinenti nel panorama dello sviluppo di software sicuro.

LEGGI LA RELAZIONE

ENISA good practices for security of Smart Cars (Buone pratiche dell'ENISA per la sicurezza delle auto intelligenti)

Buone pratiche per la sicurezza delle auto intelligenti, ovvero i veicoli connessi e (semi-) autonomi, per migliorare l'esperienza degli utilizzatori e accrescere la sicurezza delle auto .

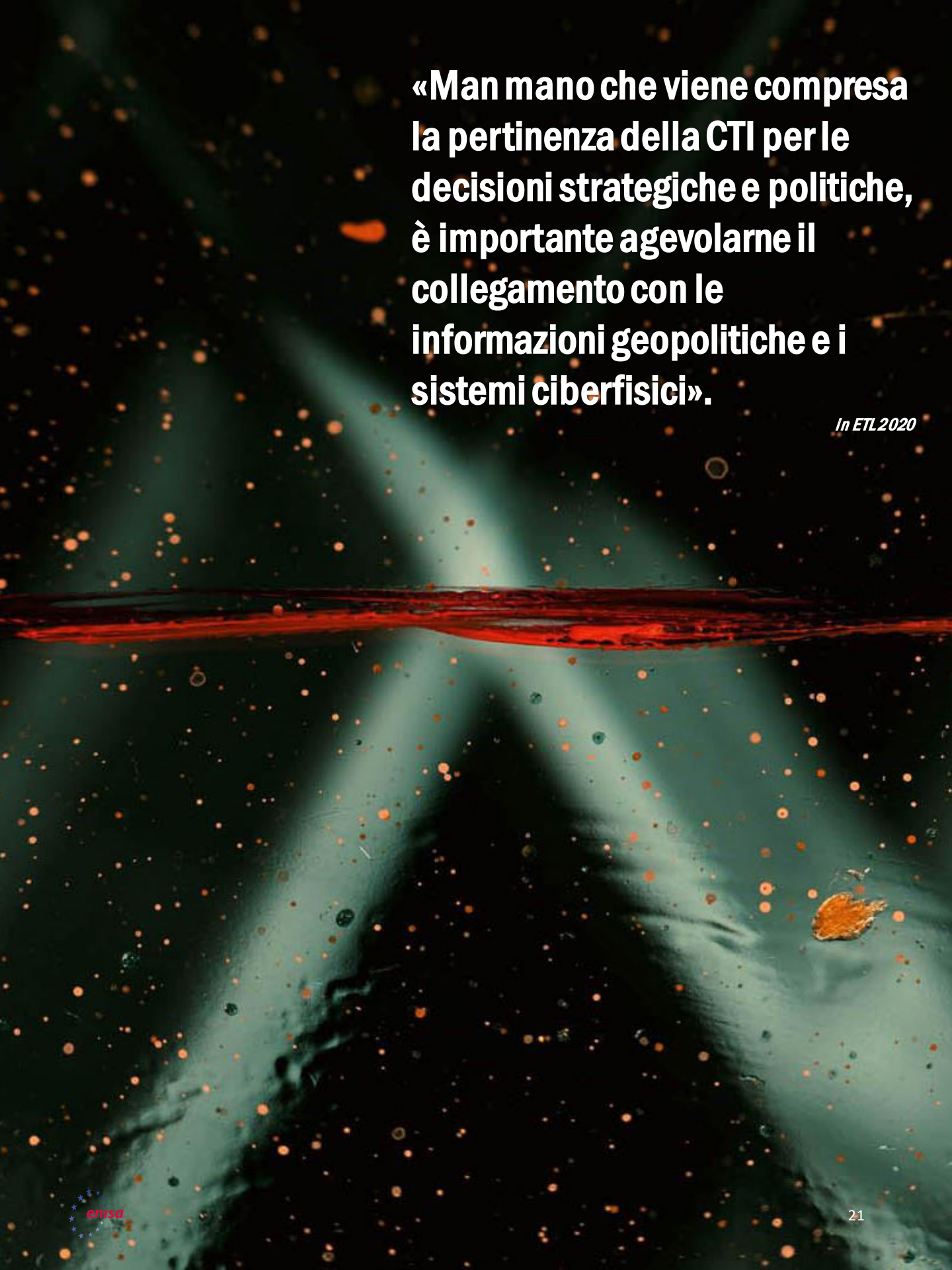
LEGGI LA RELAZIONE



Good Practices for Security of IoT - Secure Software Development Lifecycle (Buone pratiche per la sicurezza dell'Internet degli oggetti - Ciclo di vita dello sviluppo di software sicuro)

Sicurezza dell'IoT, con particolare attenzione alle linee guida di sviluppo del software.

LEGGI LA RELAZIONE



«Man mano che viene compresa la pertinenza della CTI per le decisioni strategiche e politiche, è importante agevolarne il collegamento con le informazioni geopolitiche e i sistemi ciberfisici».

in ETL 2020

Informazioni

_ L'agenzia

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'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) e Thomas Hemker.

Redattori

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

Contatti

Per informazioni sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

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

https://www.enisa.europa.eu