enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Übersicht über Cyberthreat Intelligence

ENISA Threat Landscape

Überblick

Entwicklungen im Bereich CTI

In diesem Bericht bewerten wir den Stand der Cyber Threat Intelligence (CTI) als dynamische Cybersicherheitsdomäne. Diese Analyse zielt darauf ab, die wichtigsten Trends in der raschen Entwicklung von CTI aufzuzeigen, indem relevante Referenzen bereitgestellt und die nächsten Schritte zusammengefasst werden, die erforderlich sind, um dieses Thema in den kommenden Jahren voranzutreiben.

Im Januar 2020, hat ENISA ihre **CTI-EU** Community-Bonding-Veranstaltung organisiert. Bei dieser Veranstaltung zeigten verschiedene Präsentationen den aktuellen Stand der CTI auf kommerzieller, institutioneller und Benutzerebene. Präsentationen, Diskussionen und Demonstrationen von CTI-Anbietern befassten sich mit dem Status von Produkten, Ansätzen und Praktiken und wiesen auf bestehende Probleme hin. Es ist offensichtlich, dass **CTI eine ausreichende Reife erreicht hat und jetzt eine kritische Masse an** CTI-verwandtem Material verfügbar ist, z. B. durch aktuelle Praktiken, Programme und Prozesse.

Es scheint, dass die **nächste Herausforderung bei CTI darin bestehen wird, bestehende Praktiken zu festigen, zu konsolidieren und zu verbreiten,** um eine umfassendere Nutzung auf kosteneffiziente und synergetische Weise zu erreichen. Die Hauptmöglichkeiten in dieser Hinsicht liegen im Austausch nicht wettbewerbsfähiger CTI-Praktiken, -Anforderungen, -Programme und -Informationen. Darüber hinaus werden durch die Identifizierung neuer Stakeholder, die in das CTI-Geschäft einsteigen - sowohl Hersteller als auch Verbraucher - die Funktionen verbessert, Standard-CTI-Anforderungen ermittelt und CTI-Sharing-Funktionen zeitnah eingerichtet. ENISA plant, sowohl durch ihre CTI-EU-Veranstaltung als auch durch die Zusammenarbeit mit verschiedenen EU-Interessengruppen Synergien zu stärken und bewährte CTI-Praktiken zu verbreiten.

_CTI-Instrumente, -Material und -Praktiken

Commission Horizon 2020 Forschung und Rahmen_ Verschiedene CTI-bezogene H2020-Projekte wurden abgeschlossen oder sind noch in Bearbeitung. Sie haben bereits erhebliche Mittel verbraucht und eine Vielzahl von Instrumenten und Verfahren für die Erstellung, die Anwendung und Nutzung von CTI bereitgestellt.

Praktiken von Normungsgremien, internationalen Organisationen, Regierungen, Industrie, Wissenschaft und einzelnen Anwendern_ Es wurden verschiedene bewährte Praktiken entwickelt, die Folgendes abdecken: CTI-Methoden, -Rahmen und -Verfahrensmodelle[1,2,3] Reifeprobleme, Anforderungen, Nutzererhebnungen, Bewertung von Instrumenten[8,9,10], Ansätze zur Entwicklung von CTI[11,12] usw.

Open-Source CTI-Angebote_ Verschiedene Open-Soource-Feeds[13] und Instrumente, die OpenCTI unterstützen[14], sind für Hersteller und Verbraucher wichtig und ermöglichen den freien Zugang zu wertvollen CTI zu geringen Kosten.

Open-Source CTI-Instrumente (und Praktiken)_ Es wurden zahlreiche Open-Source-Instrumente, -Praktiken und -Artikel veröffentlicht[15,16], die praktische Ansätze für die CTI-Analyse und -Verbreitung mithilfe von Open-Source-Instrumenten bieten.[17,18,19]

Überblick

_CTI Schulungsmöglichkeiten

CYBRARY_ Einführung in die Cyber Threat Intelligence.[21]

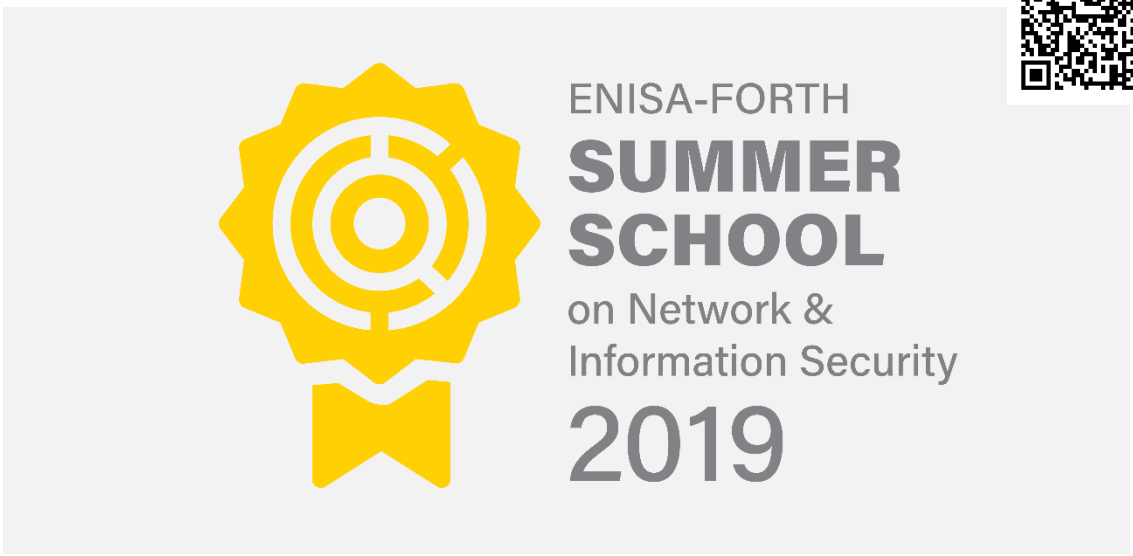
INSIKT_ Erfahren Sie mehr über die "Cyber Threat Intelligence Certification Protocols".[22]

SANS_ FOR578: Cyber Threat Intelligence.[23]

FIRST.org_ Cyber Threat Intelligence Symposium.[24]

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

ENISA-FORTH_ NIS (Netzwerk- und Informationssicherheit) Sommerschule – Cyber Threat Intelligence Training.[26]



ENISA-FORTH Summer School 2019

CTI-EU Community Event 2020

Überblick

Lücken in verfügbaren CTI-Materialien und -Praktiken

Trotz des höheren Reifegrades bei CTI-Praktiken und -Instrumenten sowie der Bereitstellung und der Anwendung von CTI bestehen immer noch Lücken bei CTI, insbesondere in Bezug auf verschiedene Anwendungsfälle, sektorale CTI und CTI-Typen (operativ, taktisch, strategisch). Eine solche signifikante Lücke wurde in der Diskussion im ENISA CTI-Forum über die Verfügbarkeit **aktueller CTI aufgrund von Angriffen** auf kritische Sektoren und kritische Dienste festgestellt. Es wurde vereinbart, dass CTI-Elemente (z. B. Tools, Techniken und Verfahren oder TTPs), die in verschiedenen internationalen bewährten Verfahren und Rahmenbedingungen (z. B. ATT&CK[28]) enthalten sind, weiterentwickelt werden müssen, um Informationen aus einem breiteren Spektrum von Angriffen einzubeziehen. Besonders dringlich sind die CTI-Elemente verschiedener Sektoren sowie Infrastrukturen und Angebote für die Bereitstellung von Diensten. Ein Beispiel dafür ist die mangelnde Betonung von **Angriffen auf Cloud-Computing**.[29] Ähnliche Anforderungen können von Infrastrukturen ausgehen, die entweder entstehen (z. B. 5G[30]), oder spezialisierter Natur sind, jedoch in kritischen industriellen Systemen eine wichtige Rolle spielen, wie beispielsweise in industriellen Steuerungssystemen (ICS) und Systeme zur Überwachung und Datenerfassung (SCADA).[31]

Obwohl vorhandene Frameworks verschiedene Elemente enthalten können, die in TTPs verwendet werden, die auf solche Systeme abzielen, muss ihre Anwendbarkeit in verschiedenen Sektoren erweitert werden, um den Besonderheiten von TTPs Rechnung zu tragen, z. B. dem Missbrauch verfügbarer APIs (Application Programming Interfaces) und der Nutzung von Kernressourcen. Abgesehen von TTPs sind weitere Leitlinien zu **Präventions-, Erkennungs- und Minderungspraktiken** für diese Sektoren erforderlich.

Dies wird die Entwicklung der erforderlichen Fähigkeiten erleichtern und den Einsatz von CTI ermöglichen, die speziell für diese Sektoren entwickelt wurden. Das Haupthindernis für die Verbreitung umsetzbarer CTI für verschiedene Plattformtypen und Infrastrukturen ist die Zeitspanne zwischen einem Vorfall, der Erstellung verwandter CTI und der Einpflegung dieser Informationen mit Open-Source-Tools. Eine **engere Koordination und Zusammenarbeit** zwischen den beteiligten Parteien wird die Zeit verkürzen, bevor CTI der breiteren Benutzergemeinschaft zur Verfügung gestellt wird. Der Aufbau von Vertrauen zwischen den teilnehmenden Unternehmen ist der Schlüssel zur Beschleunigung der CTI-Lieferkette. Die Identifizierung relevanter Akteure und die Mobilisierung der CTI-Community sind wichtig, um diese Interaktionen zu erleichtern.

Ein weiteres Hindernis für den Aufbau der erforderlichen Funktionen ist die Verfügbarkeit und die Anwendung von CTI im Rahmen verschiedener Cybersicherheitsmanagementaktivitäten. Beispiele hierfür sind im Bereich Cybersicherheit das Krisenmanagement, das Vorfallmanagement, die Reaktion auf Vorfälle, die Bedrohungserkennung und das Schwachstellenmanagement. Dieser Mangel wurde im vorherigen ENISA Threat Landscape-Bericht (ETL)[32] anhand von asynchronen Zyklen zwischen Cybersicherheitsdisziplinen bewertet und besteht weiterhin.

Abschließend sei angemerkt, dass die beschriebenen Mängel nicht auf mangelndes CTI-Wissen an sich zurückzuführen sind, sondern auf die langen sektor- und sektorübergreifenden Kommunikations- und Koordinierungszyklen für den Austausch von CTI-Wissen.

Überblick

_Probleme beim Aufbau einer CTI-Infrastruktur

CTI wird in einigen breiten Kategorien angeboten, je nach den Anforderungen der Benutzer an CTI, nämlich als operativ, taktisch und strategisch. Bestehende kommerzielle Angebote, die aus Instrumenten zur Erfassung, Wartung, Analyse und Verbreitung von CTI, CTI-Feeds, TIPs (Threat Intelligence Plattformen) usw. bestehen, unterstützen einige dieser CTI-Typen. Es gibt jedoch keinen einheitlichen Ansatz.

Bestehende Angebote konzentrieren sich auf operative und taktische CTI, während strategische CTI meist unabhängig angeboten werden.

Die Grenzen zwischen CTI sind jedoch eher verschwommen. Dies hat zur Folge, dass die Auswahl geeigneter Elemente nicht einfach ist, wenn ein CTI-Nutzer eine Fähigkeit und die entsprechende Umgebung zum Verwalten von CTI aufbauen möchte. **Dies liegt hauptsächlich daran, dass die Bereitstellung von CTI-Diensten und die vorhandene CTI-Programm-Landschaft ziemlich fragmentiert sind.** Beim Versuch, eine solche Umgebung aufzubauen, müssen CTI-Benutzer dazu ein bestes System („best of breed“) aus den vorhandenen Angeboten auswählen. Ihre Auswahl muss die CTI-Anforderungen und die angewandten CTI-Praktiken und -Prozesse erfüllen und dabei ihre aktuellen und zukünftigen CTI-Reifeziele berücksichtigen.

Obwohl einige CTI-Kriterien und -Anforderungen für verschiedene CTI-Benutzerprofile entwickelt wurden[33], sind ähnliche Anforderungen für weitere CTI-Produkte, -Dienstleistungen und -Instrumente erforderlich. Im Idealfall konzentrieren sich diese Anforderungen auf verschiedene Reifegrade der Benutzer, Ausgaben und Arten von CTI. Ähnliche Kriterien/Anforderungen sind für verschiedene andere Elemente einer CTI-Infrastruktur erforderlich, z. B. Instrumente, bewährte Verfahren, gemeinsame Nutzung von Plattformen usw.

Auf lange Sicht kann OpenCTI[14] eine gute Lösung sein, um die Probleme zu lösen, die durch die Fragmentierung von CTI-Angeboten verursacht werden, da CTI-Quellen verschiedener Typen in eine einzige Programm-Umgebung integriert werden können.

Im kommenden Jahr werden die Interessengruppen von ENISA und CTI einige Anstrengungen unternehmen, um die Anforderungen an die CTI-Infrastruktur zu bewerten und zu prüfen, wie sie von vorhandenen CTI-Produkten erfüllt werden können. Dies beginnt mit dem Versuch, eine CTI-Infrastruktur für die internen Bedürfnisse von ENISA zur Entwicklung einer CTI-Plattform für strategische CTI einzurichten.

Überblick

Effektive Nutzung von CTI in verwandten Disziplinen der Cybersicherheit

Die Einbeziehung von CTI in wichtige Disziplinen der Cybersicherheit wurde bereits von Mitgliedern der CTI-Community als Problem identifiziert. Dies ist insbesondere bei Sicherheitsmanagementaktivitäten und -komponenten der Fall, die sich auf hochdynamische Umgebungen mit erhöhter Gefährdung beziehen, wie z. B. Benutzergeräte (z. B. USIMS, Sicherheitstoken, mobile Geräte, industrielle Systeme, E-Health-Geräte usw.). Andere verwandte Disziplinen, die von CTI erheblich profitieren können, sind unter anderem Zertifizierungsaktivitäten, Krisenmanagementpraktiken, Cyber-Forensik und Reaktion auf Vorfälle.

ENISA erkennt[35] die Notwendigkeit an, **CTI in den Bereich der Zertifizierung aufzunehmen.** Im Jahr 2020 richtete die ENISA eine Ad-hoc-Arbeitsgruppe ein, die darauf abzielt, Risikomanagement und CTI in Praktiken zur Ermittlung des Sicherheitsniveaus zu integrieren.

Insbesondere stellt der CSA fest, dass „***das Sicherheitsniveau in Bezug auf die Wahrscheinlichkeit und die Auswirkungen eines Vorfalls dem Risikoniveau im Zusammenhang mit der beabsichtigten Verwendung des ICT-Produkts, des ICT-Dienstes oder des ICT-Prozesses angemessen sein muss***“ **(Art. 52(1)).**

Dies macht deutlich, dass CTI mithilfe einer Bewertung des Sicherheitsniveaus in den Zertifizierungsprozess einfließen muss. Obwohl Teile der CTI in Zertifizierungsstandards[36] unter Verwendung eines „Angreiferprofils“ vorgesehen sind, umfasst dieses Konzept einen kleinen Teil der verfügbaren CTI.

Die Arbeit der **Ad-hoc-Arbeitsgruppe von ENISA** besteht darin, Informationen aus Risiko- und Bedrohungsbewertungen (CTI) zu kombinieren, um die Anforderungen an den Gruppenschutz angemessen zu erfüllen und sie auf verschiedene Sicherheitsebenen abzubilden. Die Kartierung wird auf verschiedenen Risikostufen basieren, die sich aus der Gefährdung von Vermögenswerten ergeben, und gleichzeitig Vorschläge für die Anzahl und Stärke der Minderungskontrollen liefern. Diese Kontrollen werden die Auswahl von Sicherheitsfunktionen vorantreiben, die mehreren Sicherheitsstufen zugewiesen werden und hängen von der Implementierung durch die verschiedenen Zielinstanzen für die Zertifzierung (ToCs) ab.

Die Arbeit von ENISA zu diesem Thema wird mit Unterstützung einer Expertengruppe durchgeführt, die Risikomanagement-, CTI- und Zertifizierungskompetenzen kombiniert. Die Arbeit startete im April 2020 und sollte im dritten Quartal 2020 enden. Die Ergebnisse dieser Arbeit werden von ENISA veröffentlicht.

Überblick

_Ergebnisse einer umfassenden CTI-Umfrage

Aus einer repräsentativen CTI-Umfrage[7] können zahlreiche interessante Schlussfolgerungen zur aktuellen Akzeptanz von CTI-Praktiken und -Instrumenten gezogen werden. Die Umfrage spiegelt unter anderem den aktuellen Stand der CTI-Funktionen, die bei den Stakeholdern verwendeten CTI-Typen, das Zusammenspiel der CTI-Praktiken mit anderen Prozessen in Organisationen und die Anwendungsfälle von CTI-Programmen wider.

In dieser Diskussion werden die Ergebnisse der Umfrage auf die Erfahrungen der ENISA im Rahmen ihrer eigenen (strategischen) CTI-Aktivitäten und auf die Rückmeldungen verschiedener CTI-Interessenvertreter innerhalb der EU und der europäischen CTI-Foren[36] hochgerechnet. In diesem Zusammenhang liegt der Schwerpunkt auf der Identifizierung von Anforderungen, dem Sammeln von Informationen, der Erstellung strategischer CTI, dem Einsatz von Programmen und Praktiken und der Integration in andere relevante Prozesse. In diesem Zusammenhang möchten wir die folgenden Punkte hervorheben.

- Eine der wichtigsten Schlussfolgerungen aus diesem Bericht ist, dass die **Halbautomatisierung der CTI-Produktion** ein wichtiges Instrument ist: Während die Automatisierung der Informationsaufnahme zunimmt - trotz eines Anstiegs der CTI-Nutzung durch Anbieter - bilden manuelle Aktivitäten immer noch den Kern der CTI-Produktion von Unternehmen.

- Die Aktivitäten zur Aggregation, Analyse und Verbreitung von Informationen werden mithilfe **weit verbreiteter Instrumente** wie Tabellenkalkulationen, E-Mail- und Open-Source-Verwaltungsplattformen verwaltet, was auf die Effizienz kostengünstiger Lösungen hinweist.

- Die Bedeutung der Definition von **CTI-Anforderungen** wird von der CTI-Benutzergemeinschaft verstanden. Dies ist eine Reaktion auf die wiederholten Bitten von CTI-Experten[5,6], die Bedeutung der CTI-Anforderungen anzuerkennen, und zeigt, dass die CTI-Community ihren Rat befolgt hat. Es ist auch interessant zu sehen, dass ein erheblicher Teil der CTI-Anforderungen die Bedürfnisse von Unternehmen und Führungskräften widerspiegelt. Dies ist ein Hinweis darauf, dass CTI Teil der Entscheidungsfindung auf Geschäfts- und Managementebene wird.
- Eine Kombination aus Verbrauch und Produktion von CTI ist die vorherrschende Methode zum Aufbau einer internen **CTI-Wissensbasis**. Eine Steigerung der CTI-Produktion von Unternehmen ist der Haupttrend, insbesondere für CTI, die aus ihrer eigenen Analyse von Rohdaten und kontextualisierten Bedrohungswarnungen abgeleitet wurden. Die Anwendung aus öffentlich zugänglichen Quellen wird angesichts der zunehmenden Verwendung verfügbarer CTI (Open-Source-CTI-Feeds, wie im folgenden Punkt angegeben) zu einem Trend.
- **Das Sammeln von Open-Source-Informationen** ist die am häufigsten verwendete Aufnahmemethode, gefolgt von Bedrohungs-Feeds von CTI-Anbietern. Dies ist ein klarer Aufwärtstrend im Jahr 2020, der darauf hinweist, dass CTI-Benutzer in ihre eigenen Fähigkeiten investieren, um CTI zu produzieren, die ihren Anforderungen entspricht.
- Die **Erkennung von Bedrohungen** wird als Hauptanwendungsfall für CTI bewertet. Obwohl Kompromittierungsindikatoren (IoCs) nach wie vor die wichtigsten Elemente der CTI bei der Erkennung von Bedrohungen und der Reaktion auf Bedrohungen sind, scheinen das Bedrohungsverhalten und die gegnerische Taktik (TTPs) für Aufwärtstrends bei der Verwendung von CTI in Organisationen verantwortlich zu sein.
- Die Messung der **Effektivität von CTI** ist immer noch eine schwierige Aufgabe, und nur ein kleiner Prozentsatz der CTI-Benutzer (4 %) implementiert Prozesse zur Messung der CTI-Effizienz. Es wird argumentiert, dass Tools zwar einen Mehrwert für die CTI-Analyse bieten können, die Fähigkeiten des Analysten jedoch für die erfolgreiche Implementierung von CTI am wichtigsten sind. Ein interessantes Ergebnis in Bezug auf die Zufriedenheit ist die niedrige Bewertung des Werts der Funktionen des maschinellen Lernens.

Überblick

Schlussfolgerungen und nächste Schritte

In Anbetracht all dieser Entwicklungen im Bereich CTI können die folgenden Schlussfolgerungen gezogen werden. Aus diesen Schlussfolgerungen ergeben sich einige weitere Schritte, zumindest aus Sicht der ENISA, bei denen CTI gemäß ihrem neuen Mandat gestärkt wird, aber auch die in den Communities ihrer Interessengruppen, wie zum Beispiel den Mitgliedstaaten, der Europäischen Kommission und anderen europäischen Einrichtungen, Anbietern und CTI-Endnutzern beobachteten Entwicklungen berücksichtigt werden:

- Angesichts der zunehmenden Zahl von Interessengruppen der EU und der Mitgliedstaaten, ist die **Zusammenarbeit und Koordinierung der EU-weiten CTI-Aktivitäten** von zentraler Bedeutung. Der Aufbau von Synergien kann zwar die CTI-Kosten senken, erhöht aber auch das Vertrauen der CTI-Akteure und ermöglicht so den Austausch von CTI und bewährten Verfahren. ENISA wird die Zusammenarbeit mit verschiedenen Interessenvertretern fördern, indem die **Ermittlung der CTI-Anforderungen** eingeleitet wird. Dies wird mehrere Interessengruppen innerhalb des EU-Ökosystems von Organisationen umfassen (d. h. Kommission, EU-Gremien, Agenturen und Mitgliedstaaten).
- Da die Relevanz von CTI für die strategische und politische Entscheidungsfindung erkannt wurde, ist es wichtig, die **Verbindung zu geopolitischen Informationen und cyber-physischen Systemen zu erleichtern.** Auf diese Weise kann die Aufnahme von CTI in Entscheidungsfindungsprozesse ermöglicht werden, und der Kontext kann zudem erweitert werden, um hybride Bedrohungen zu identifizieren.

- **Die Integration von CTI in Sicherheitsmanagementprozesse** wird dazu beitragen, dass sich CTI in verwandten Bereichen durchsetzt und zur rechtzeitigen Identifizierung, Erkennung und Verhinderung von Bedrohungen beiträgt. Eine unmittelbare Wirkung wird darin bestehen, die Agilität ziemlich langlebiger Prozesse (z. B. Zertifizierung, Risikobewertung) zu erhöhen. Gleichzeitig wird CTI die Entscheidungsfindung in Notfällen (z. B. Krisenmanagement) erleichtern, indem Beweise für die Exposition gegenüber Cyber-Bedrohungen vorgelegt werden.
- Um besser auf die zunehmende Rolle von CTI reagieren zu können, wird ENISA daran arbeiten, ein **umfassendes CTI-Programm aufzubauen.** Das ENISA CTI-Programm wird interne Fähigkeiten horizontal bündeln, um alle entsprechenden Interessenvertreter in allen Phasen der CTI-Produktion und -Verbreitung einzubeziehen und eine CTI-Infrastruktur zu entwickeln, die sowohl für interne als auch für Schulungszwecke verwendet wird.
- Investitionen in einige grundlegende CTI-Konzepte, insbesondere in **CTI-Reifegrade und Bedrohungshierarchien**, werden für eine vermehrte Einführung von CTI sehr nützlich sein. ENISA wird - zusammen mit ihren EU-Partnern - einige Anstrengungen in die Entwicklung eines CTI-Reifegradmodells investieren. Darüber hinaus konsolidiert und verbreitet ENISA nützliches Mehrzweck-CTI-Material wie Bedrohungshierarchien, die auch in anderen Bereichen verwendet werden können (z. B. Zertifizierung, Risikomanagement, sektorale Landschaften usw.).

Einige der oben genannten Schlussfolgerungen und nächsten Schritte werden in den kommenden Jahren Gegenstand der Arbeit von ENISA im Bereich CTI sein.[35]

Literaturangaben

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

2. "5-Step process to power your Cyber Defense with Cyber Threat Intelligence". 12. März 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. September, 2019. SANS, https://www.youtube.com/watch?v=J7e74QLVxCk

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

7. "2020 SANS Cyber Threat Intelligence (CTI) Survey". 10. Februar, 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. September, 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. Oktober, 2019. DNS Stuff. https://www.dnsstuff.com/what-is-threat-intelligence

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

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

13. "A List of the Best Open Source Threat Intelligence Feeds". 4. März 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. März 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. Dezember 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" Januar 2020. NetScope. https://www.enisa.europa.eu/events/2019-cti-eu/presentations/the-cti-cloud-context-dilema

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

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

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

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

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

35. "EU Cybersecurity Act" 7. Juni, 2019. Amtsblatt der Europäischen Union. 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

Themenbezogen

ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

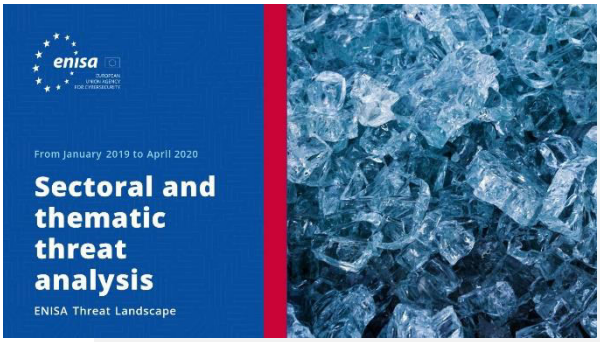
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape-Bericht
Hauptvorfälle in der EU und weltweit

Die bedeutendsten Cybersicherheitsvorfälle zwischen Januar 2019 und April 2020.

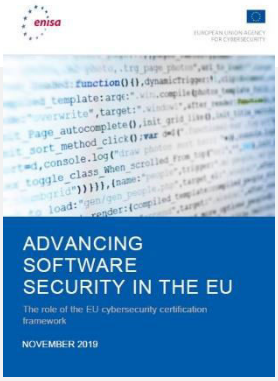
LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

Sonstige Publikationen



Verbesserung der Software-Sicherheit in der EU

Präsentiert Schlüsselelemente der Software-Sicherheit und bietet einen kurzen Überblick über die wichtigsten vorhandenen Ansätze und Standards in der sicheren Software-Entwicklungslandschaft.

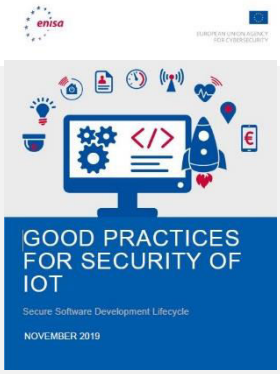
LESEN SIE DEN BERICHT

Beste Praxis der ENISA für die Sicherheit von Smart Cars

Gute Praktiken für die Sicherheit intelligenter Fahrzeuge, nämlich vernetzte und (halb-) autonome Fahrzeuge, um die Erfahrung der Fahrzeugbenutzer zu verbessern und die Fahrzeugsicherheit zu verbessern

.

LESEN SIE DEN BERICHT



Gute Praktiken für die Sicherheit von IoT - Sicherer Softwareentwicklungszyklus

ioT-Sicherheit mit besonderem Schwerpunkt auf Richtlinien für die Softwareentwicklung.

LESEN SIE DEN BERICHT

„Da die Relevanz von CTI für die strategische und politische Entscheidungsfindung erkannt wurde, ist es wichtig, die Verbindung zu geopolitischen Informationen und cyber-physischen Systemen zu erleichtern.“

In ETL 2020

Über

Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

HERAUSGEBER

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

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.

Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

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

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
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