Konferencja

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA.

ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 07 sierpnia 2020 r.

Sesja 3

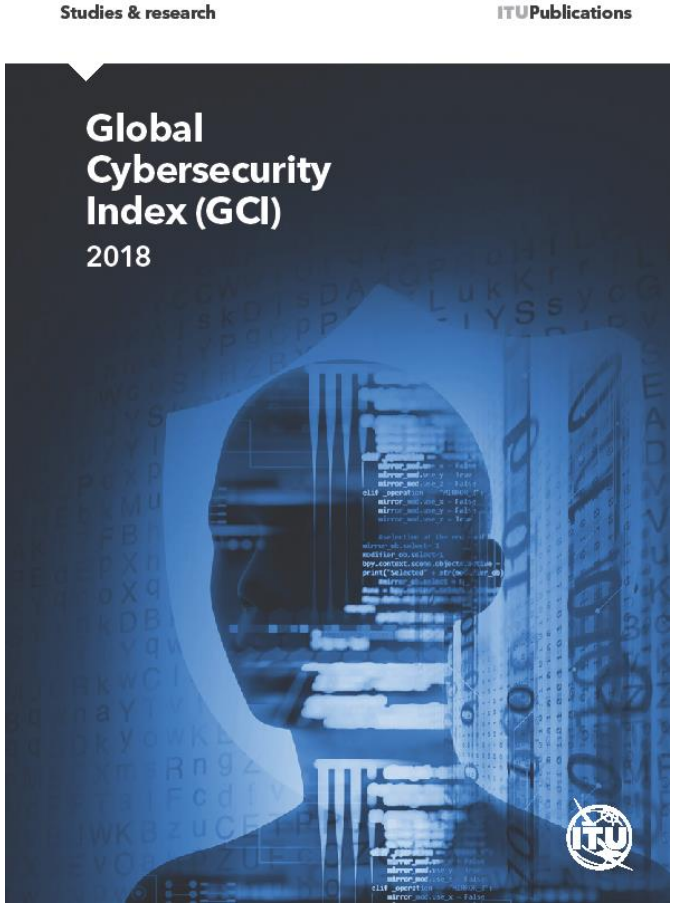
BADACZE CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo w badaniach z zakresu nauk ścisłych i technicznych

dr hab. inż. Maciej Kiedrowicz, maciej.kiedrowicz@wat.edu.pl

Wojskowa Akademia Techniczna, Wydział Cybernetyki

Opracowania ITU (International Telecommunication Union)

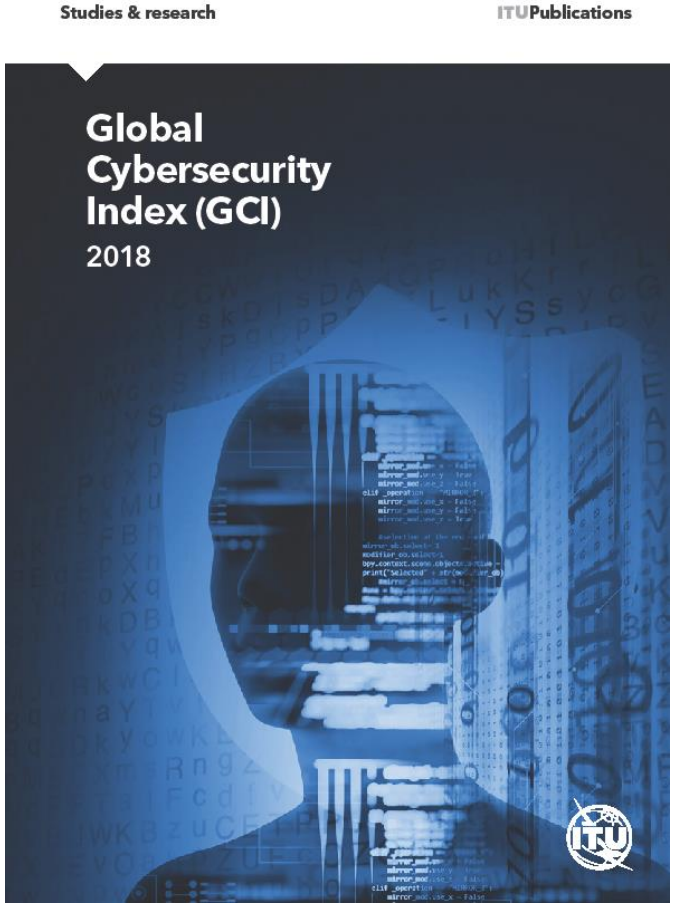


Międzynarodowa Unia Telekomunikacyjna, w ramach współpracy w zakresie cyberbezpieczeństwa, ma na celu budowanie synergii między obecnymi i przyszłymi inicjatywami narodowymi i koncentruje się na następujących pięciu filarach:

- **Prawne:** Działania oparte na istnieniu zasad (ram) oraz instytucji prawnych zajmujących się cyberbezpieczeństwem i cyberprzestępczością.
- **Techniczne:** Działania oparte na istnieniu zasad (ram) oraz instytucji technicznych zajmujących się cyberbezpieczeństwem.
- **Organizacyjne:** Działania oparte na istnieniu instytucji koordynujących politykę i strategie rozwoju cyberbezpieczeństwa na poziomie krajowym.
- **Budowanie zdolności:** Działania oparte na istnieniu programów badawczo-rozwojowych, edukacyjnych i szkoleniowych, certyfikowanych specjalistów i agencji sektora publicznego wspierających budowanie odpowiednich kompetencji.
- **Współpraca:** Działania oparte na istnieniu partnerstw, struktur współpracy i sieci wymiany informacji.

ISBN: 978-92-61-28201-1

WSKAŹNIKI:



Legal

Cybercrime legislation
Cybersecurity regulation
Containment/curbing of spam legislation

Technical Measures

CERT/CIRT/CSIRT
Standards Implementation Framework
Standardization Body
Technical mechanisms and capabilities deployed to address Spam
Use of cloud for cybersecurity purpose
Child Online Protection mechanisms

Organizational Measures

National Cybersecurity Strategy
Responsible Agency
Cybersecurity Metrics

Capacity Building Measures

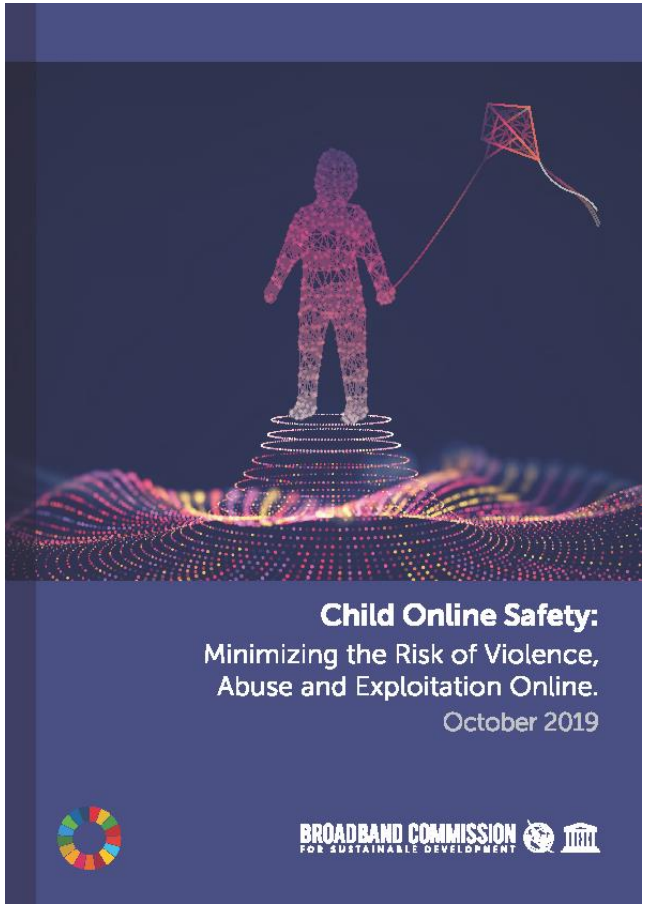
Public awareness campaigns
Framework for the certification and accreditation of cybersecurity professionals
Professional training courses in cybersecurity
Educational programs or academic curricular in cybersecurity
Cybersecurity R&D programs
Incentive mechanisms

Cooperation Measures

Bilateral agreements
Multilateral agreements
Participation in international fora/associations
Public-Private Partnerships
Inter-agency/intra-agency partnerships
Best Practices

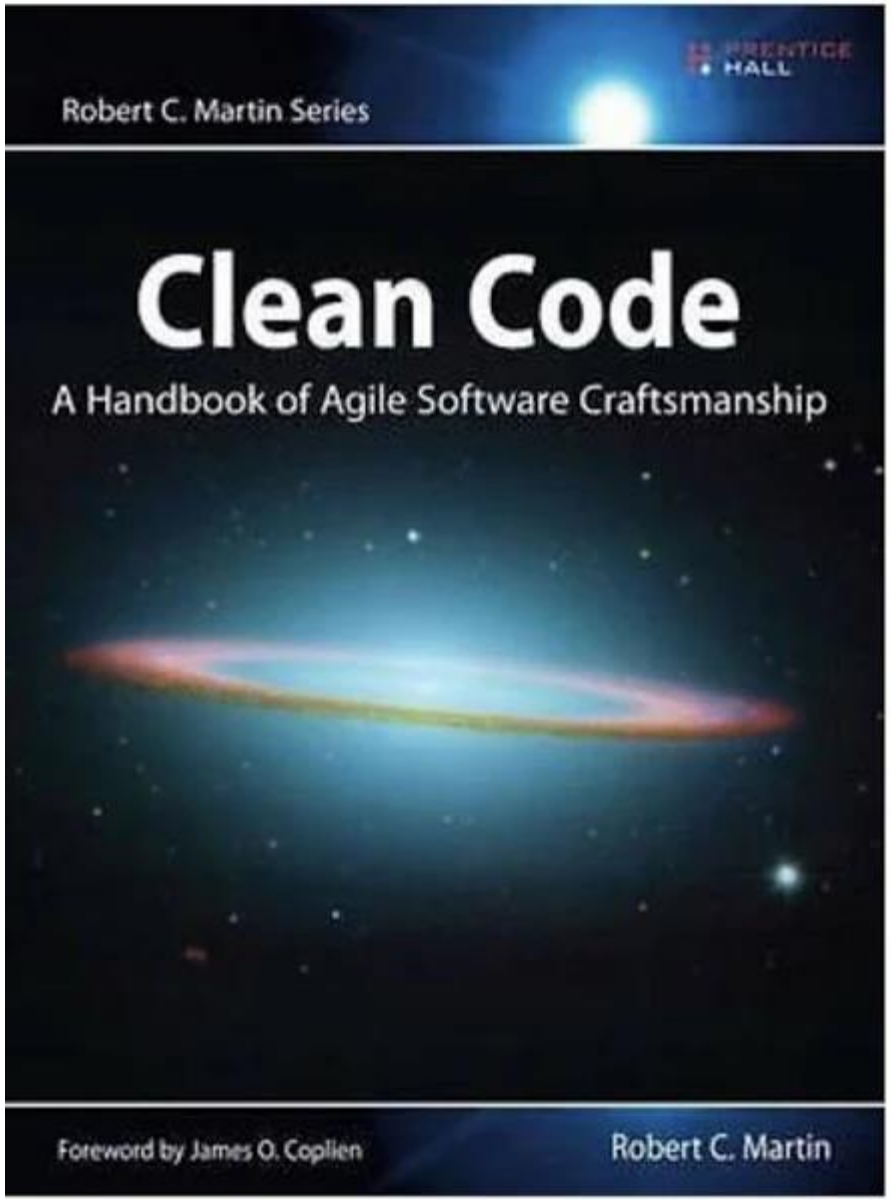
OPRACOWANIE KRAJOWEJ STRATEGII CYBERBEZPIECZEŃSTWA, PRZEWODNIK

ISBN: 978-92-61-27791-8



BEZPIECZEŃSTWO DZIECKA W INTERNECIE - MINIMALIZACJA RYZYKA PRZEMOCY, NADUŻYĆ I WYKORZYSTANIA W INTERNECIE

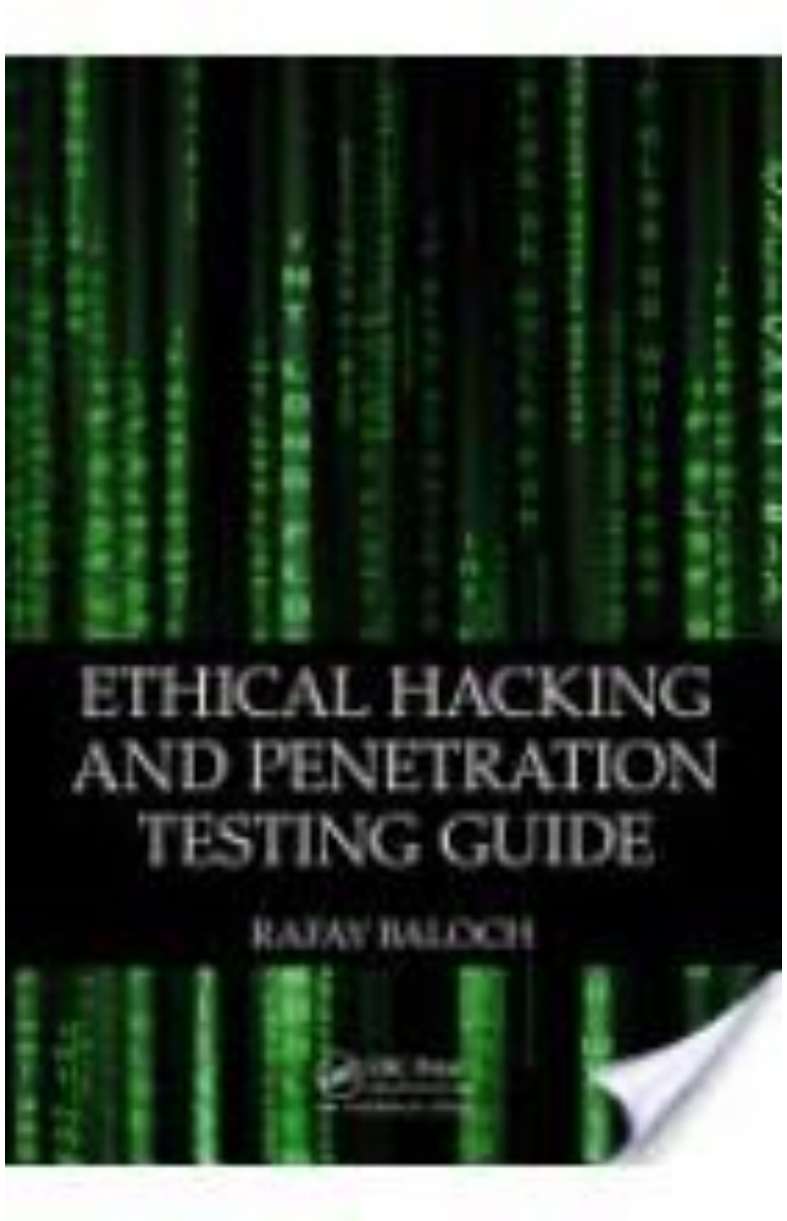
RAPORT - 2019



Clean Code
A Handbook of Agile Software

Autor: Robert Martin

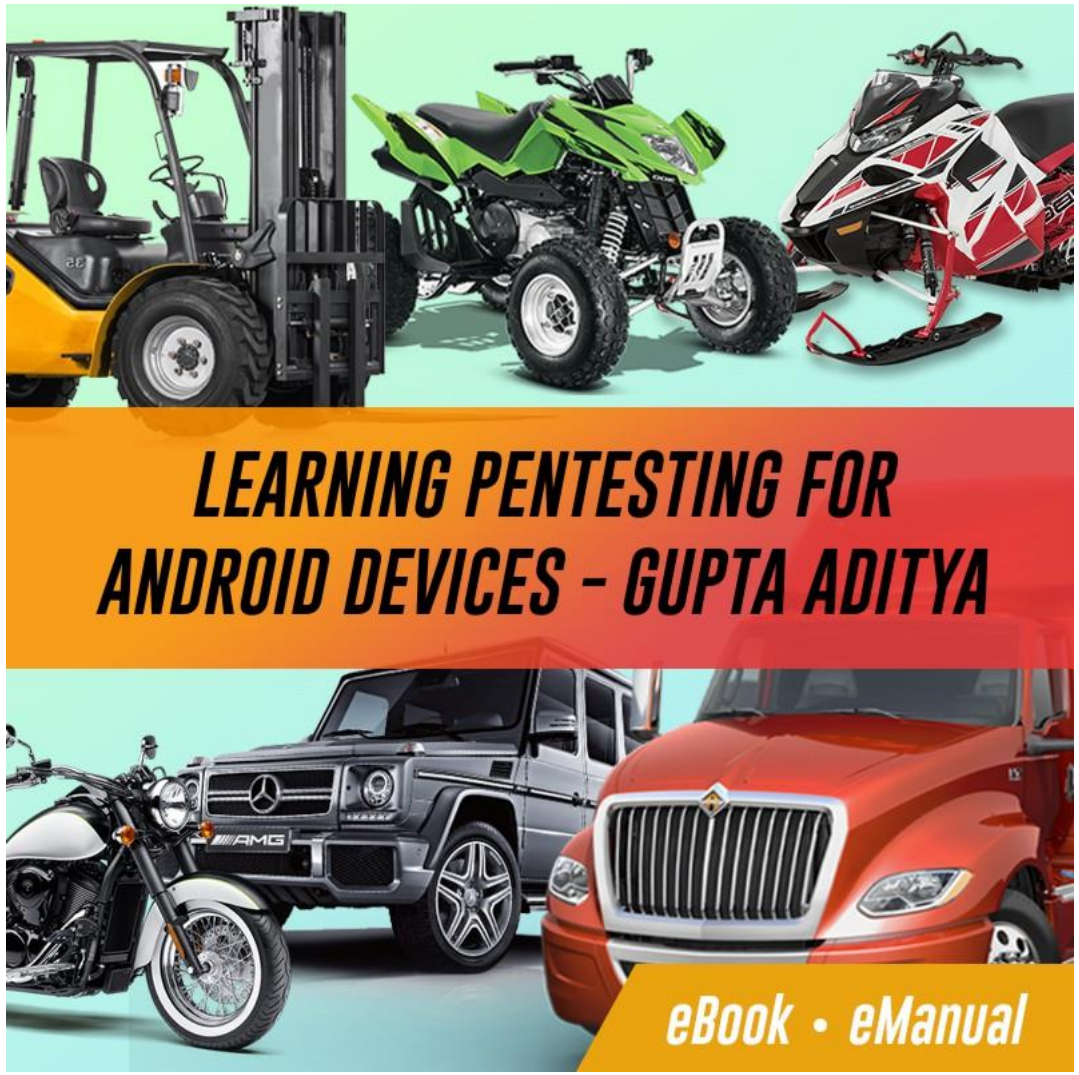
Język: Angielski
Oprawa: Miękka
Liczba stron: 464
EAN: 9780132350884
ISBN: 0132350882



Ethical Hacking and Penetration Testing Guide

Autor: Baloch Rafay

Język: Angielski
ISBN13 (EAN): 9781482231618
Kategorie: Computer fraud & hacking
Liczba stron: 531
Wydawca: Taylor & Francis
Rok wydania: 2014
ISBN10: 1482231611



Learning Pentesting for Android Devices

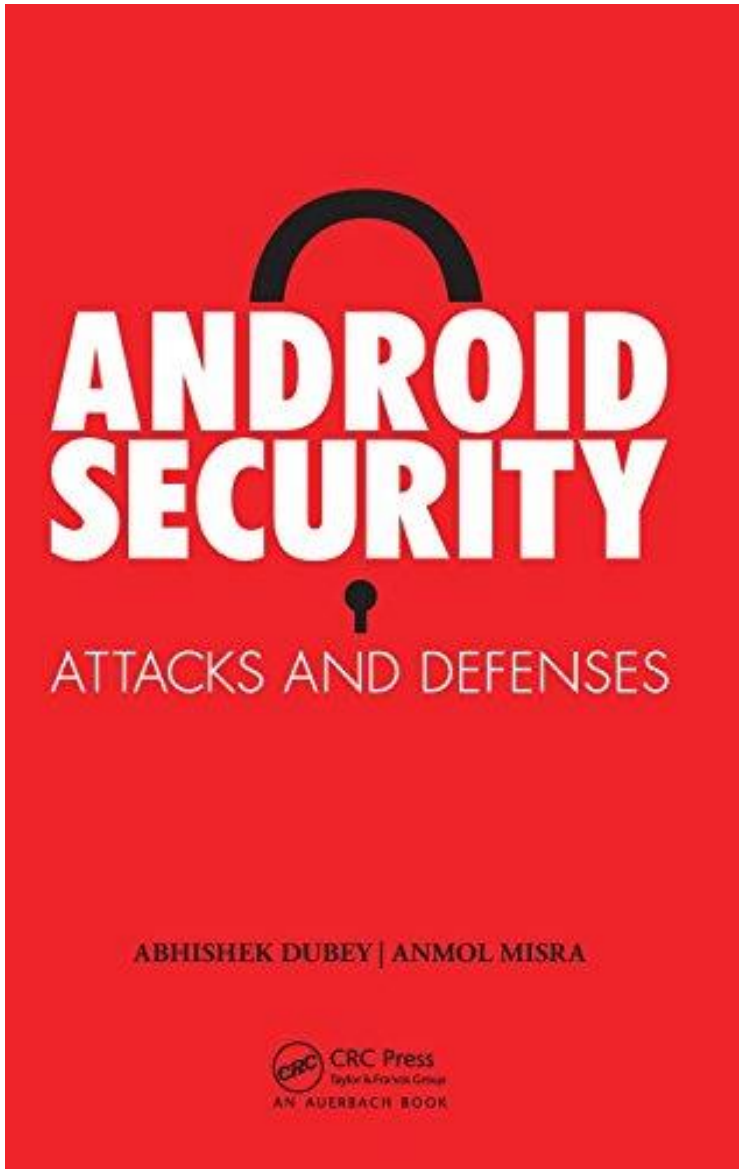
Autor: Gupta Aditya

Publisher: Packt Publishing
Language: ENG
Pages: 154
On Sale: 2014-03-26
SKU-13/ISBN: 9781783288984

Art of Software Security Assessment
Identifying and Preventing Software Vulnerabilities

Autor: Dowd Mark

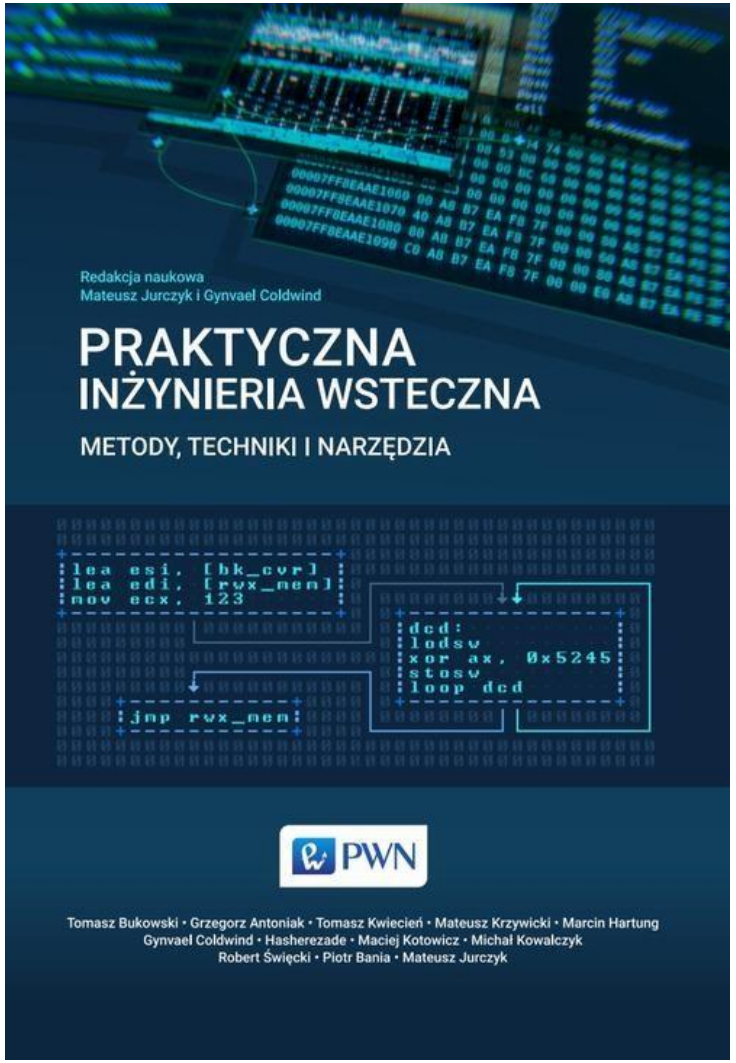
Język: Angielski
ISBN13 (EAN): 9780321444424
Liczba stron: 1200
Wydawca: Pearson Education (US)
Rok wydania: 2006



Android Security: Attacks and Defenses

Autor: Anmol Misra

Język: angielski
ISBN-13: 9781439896464
Rok wydania: 2013
Ilość stron: 280

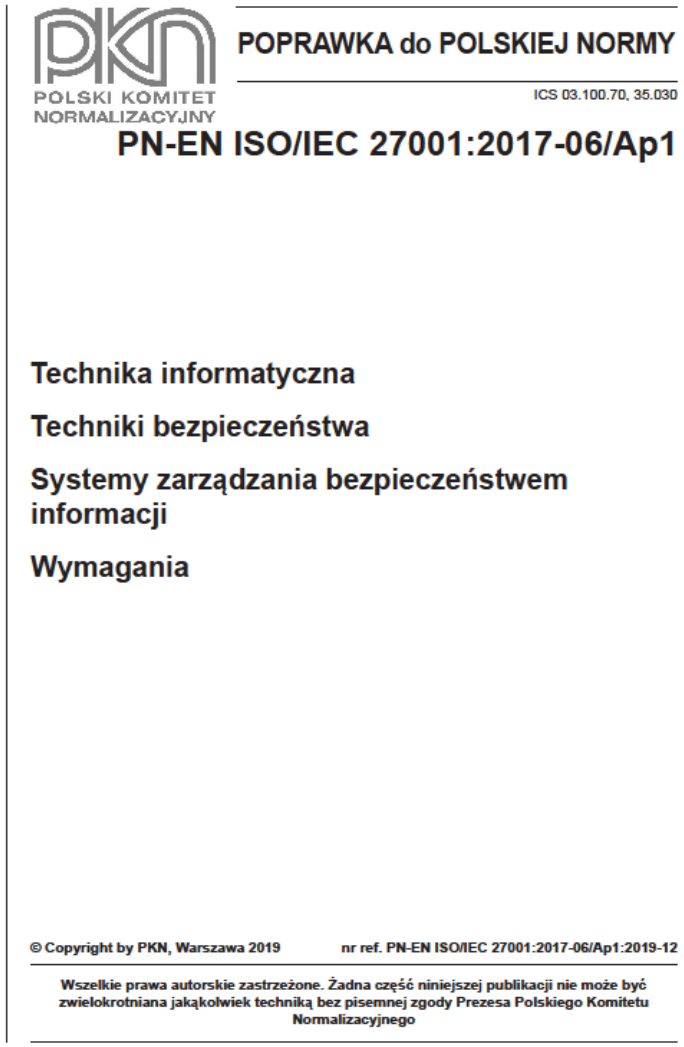


Praktyczna inżynieria wsteczna
Metody, techniki i narzędzia

Redakcja naukowa: Gynvael Coldwind, Mateusz Jurczyk

Wydawca: Wydawnictwo Naukowe PWN
ISBN: 9788301189518
EAN: 9788301189518

Liczba stron: 526



POLSKI KOMITET NORMALIZACYJNY

POPRAWKA do POLSKIEJ NORMY

ICS 03.100.70, 35.030

PN-EN ISO/IEC 27001:2017-06/Ap1

Technika informatyczna

Techniki bezpieczeństwa

Systemy zarządzania bezpieczeństwem informacji

Wymagania

PN-EN ISO/IEC 27001:2017-06 - wersja polska

Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania

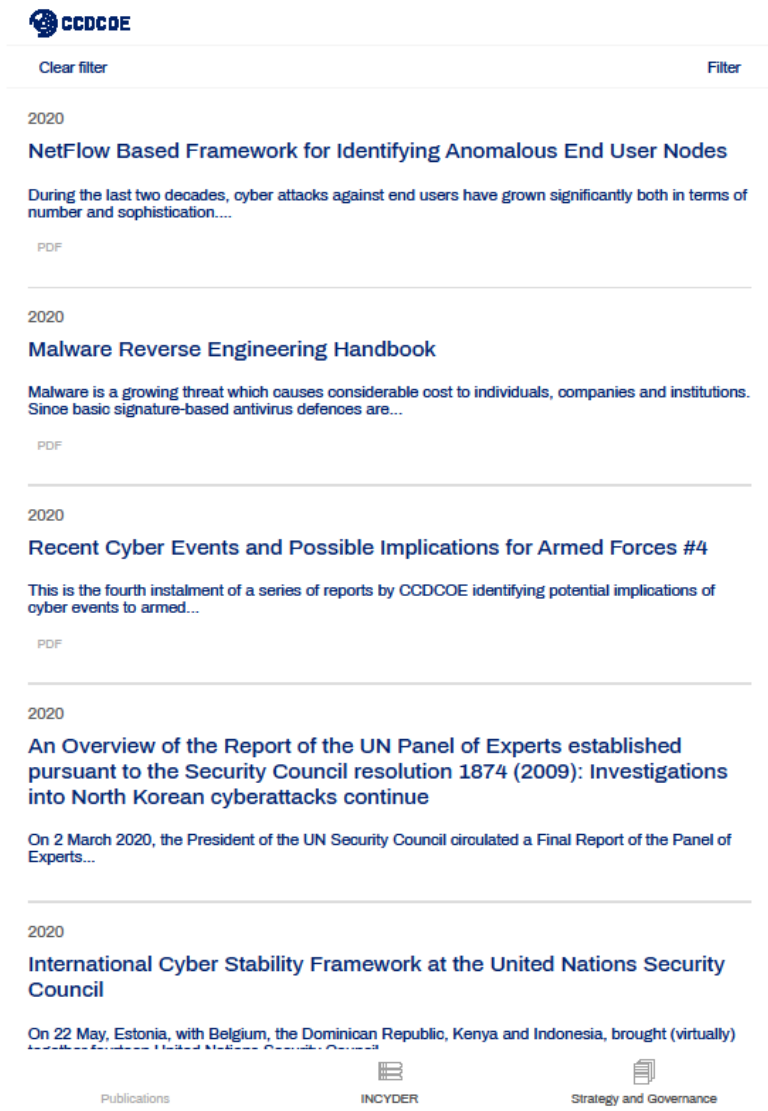
Zakres

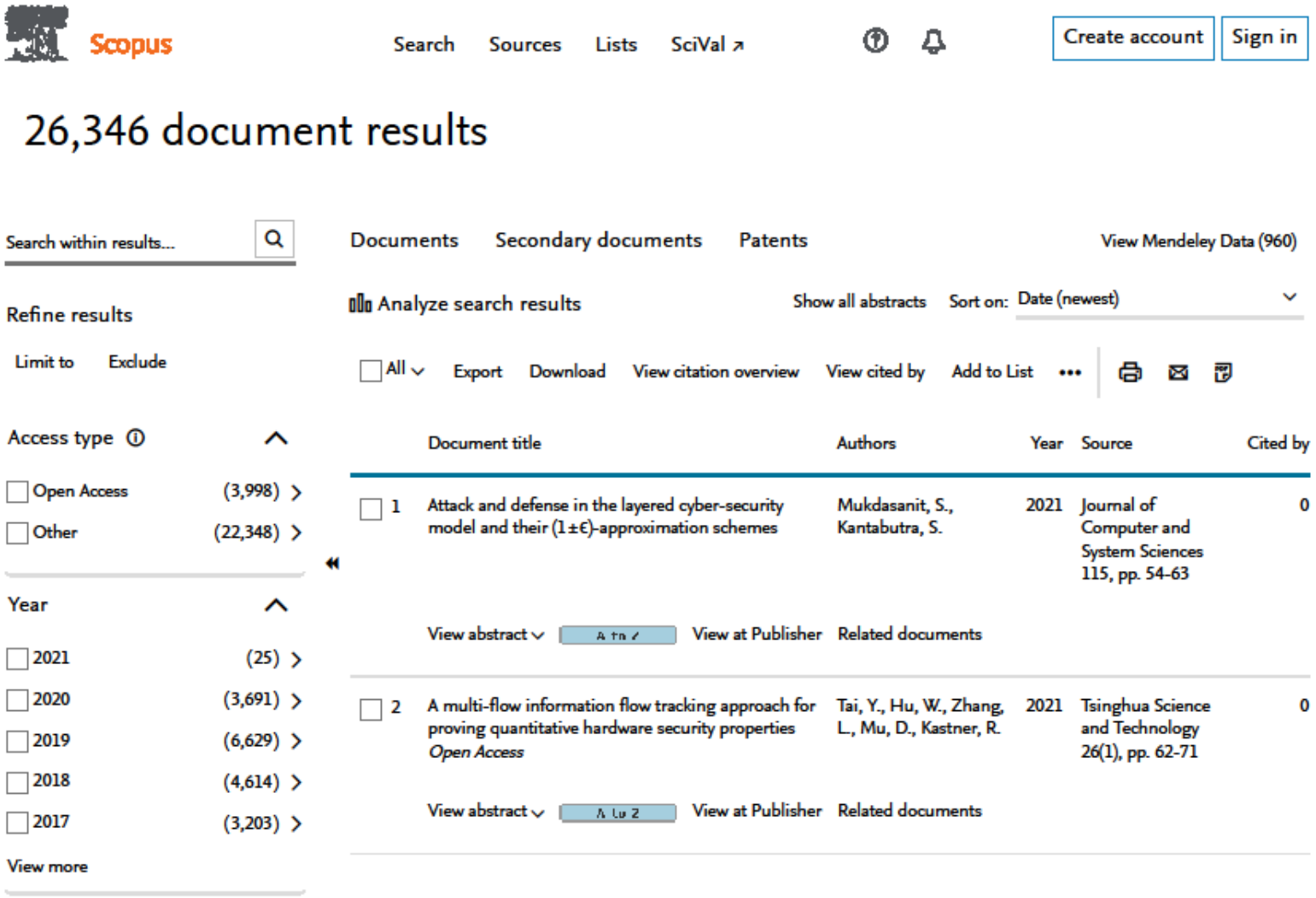
Niniejsza Norma Międzynarodowa określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania **bezpieczeństwem informacji** w odniesieniu do organizacji. Niniejsza Norma Międzynarodowa obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym **bezpieczeństwa informacji**, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej Normie Międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru. Wyłączenie któregokolwiek z wymagań określonych w Rozdziałach 4 do 10 jest nieakceptowalne, w wypadku gdy organizacja deklaruje zgodność z niniejszą Normą Międzynarodową.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

https://ccdcoe.org/library/publications/

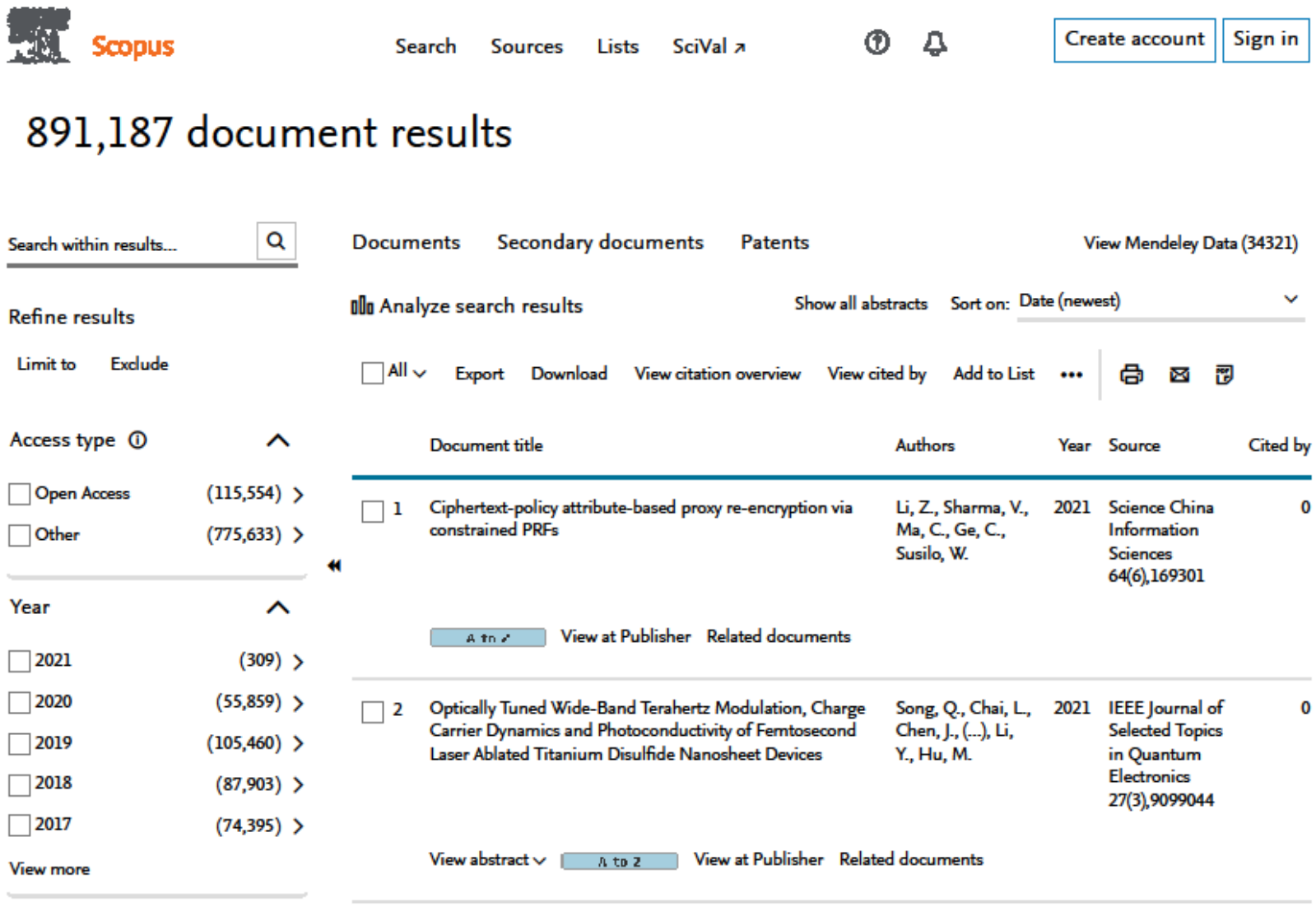
About us
As the NATO-accredited cyber defence hub we support our member nations and NATO with cyber defence expertise. CCDCOE embodies and fosters cooperation of like-minded nations
The heart of the Centre is a diverse group of experts from 25 nations: Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. We bring together researchers, analysts and educators from the military, government, academia and industry





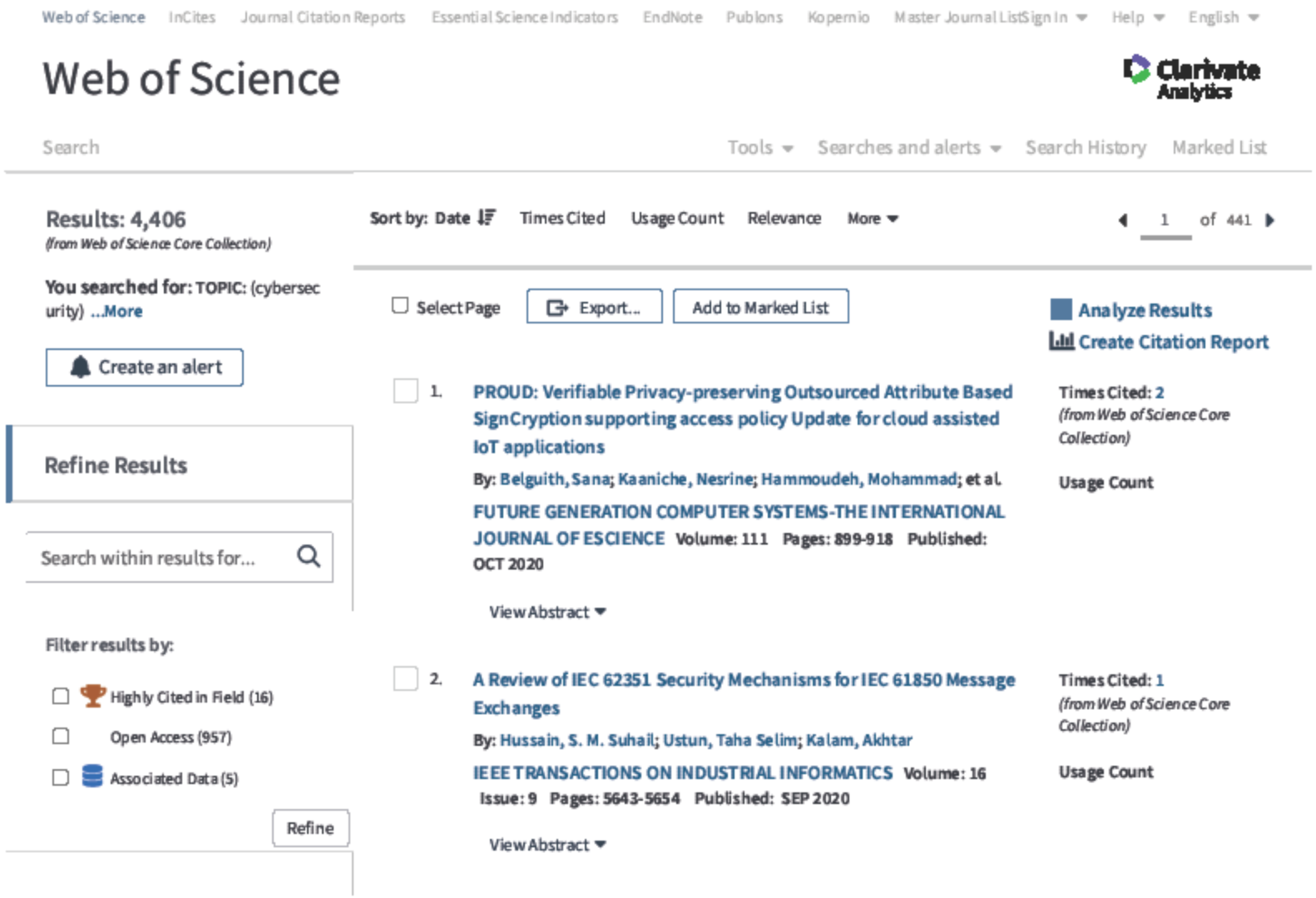
SCOPUS

cybersecurity



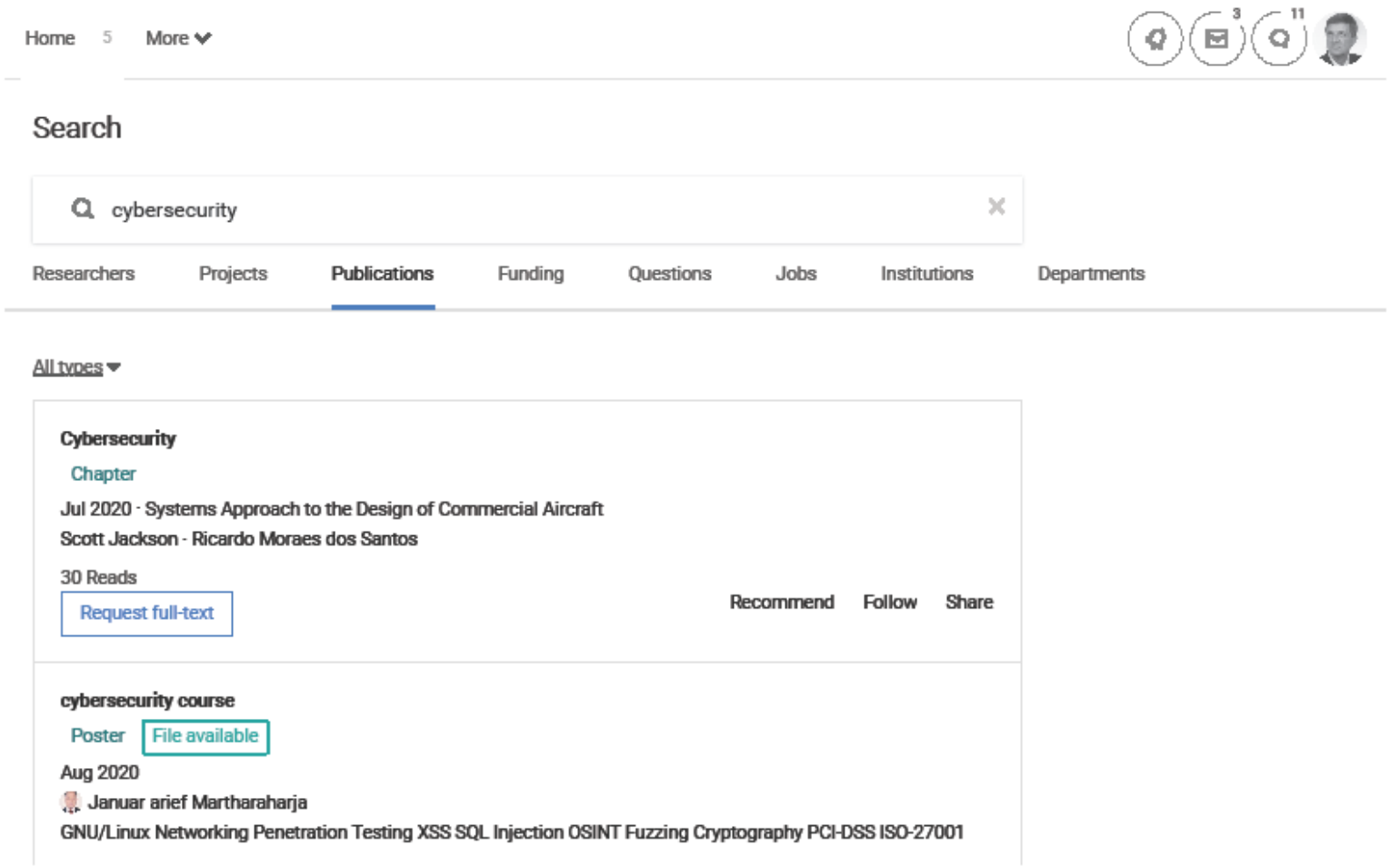
SCOPUS

information security



Web of Science

cybersecurity



Researchgate

https://www.researchgate.net/

Konferencja

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA.

ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Dziękuję za uwagę …