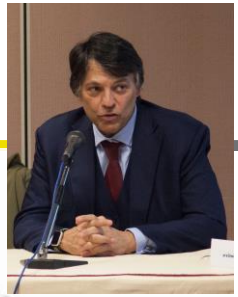
#A CYBER JOURNEY

Nicola Sotira

28 Febbraio 2024

/usr/bin/whoami



Head of Poste Italiane's CERT, he has more than two decades of experience in the field of IT and network security. His expertise has been honed in diverse international contexts, including contributions to cryptography and infrastructure security, as well as work within the mobile and 3G network domains. Furthermore, he has served as a journalist, collaborating with numerous IT sector magazines to widely disseminate knowledge on security and technical-legal aspects. Since 2004, he has been an active member of the Association for Computing Machinery (ACM) and has also played a crucial role in partnering with multiple startups in both Italy and other countries.

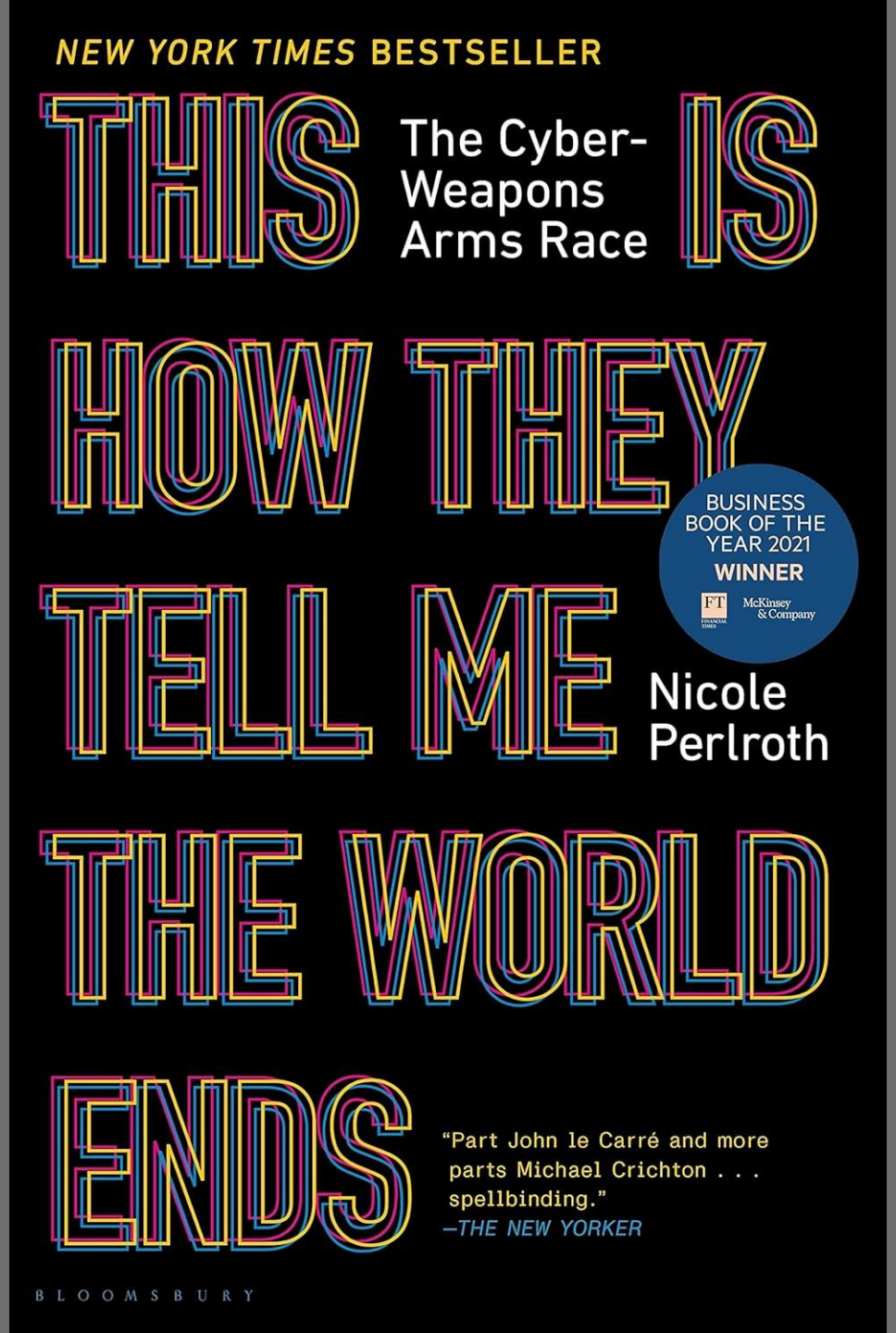
STILL A CHALLENGE…


#HUMAN


MIKKO HYPPONEN
IF IT'S SMART, IT'S VULNERABLE
WILEY
#VULNERABILITIES

#Barbarian

(*The Darkness 2015*)



NICOLE PERLROTH

Zero day: a software bug that allows a hacker to break into your devices and move around undetected. One of the most coveted tools in a spy's arsenal, a zero day can silently spy on your iPhone, dismantle the safety controls at a chemical plant, alter an election, and shut down the electric grid.

For decades, under cover of classification levels and non-disclosure agreements, the United States government became the world's dominant hoarder of zero days. U.S. government agents paid top dollar,first thousands, and later millions, to hackers willing to sell their lock-picking code and their silence.


RANSOMWARE
RANSOMWARE
RANSOMWARE

FOUR MAIN POINTS OF VIEW WHEN AI MEETS CYBER

AI USED BY ATTACKERS

- Force multiplier
- More targeted
- Increase success rate [test before you do]
- New attacks forms

HOW TO SECURE AI USAGE IN MY COMPANY

- Govern access to AI services and data
- Secure AI pipeline
- New things: secure prompts, prevent poisoning, secure the AI models

AI USED FOR DEFENSE

- Force multiplier
- Precision
- New interface, conversational & generative
- New ways to defend, better operations

AND THEN…

Like every organization, your team can leverage AI and be better

- More efficient, better operations & quality, growth, development and more

CERT

CERT

Story

Established in 2013, it has become a leading force in preventing and combating cybercrime.

Costituency

Composed of all Poste Italiane Group companies and its customers

Team

Industry experts, technicians, and analysts of the highest profile

Mission

Coordinate and neutralize cyber threats while monitoring and responding to security incidents and attacks.

ACCREDITATIONS AND CERTIFICATIONS

- Accredited in the network of European Trusted Introducer CERTs
- Membership of the Strategic and Steering Committee of the Financial CERT.
- Affiliato al Forum of Incident Response and Security Teams.
- Agreement to be signed by 2019 with Israeli CERT
- ISO 27001:2013 certified on all core services
- Among the 16 Italian CERTs surveyed by the European Agency on Network and Information Security.

We are sponsor for

LEONARDO

INTESA SANPAOLO

BANCA D'ITALIA

enav

1 COOPERATION

Università degli Studi Cagliari
Università della Calabria
Università degli Studi Mediterranea di Reggio Calabria
Polizia di Stato – Servizio Polizia Postale e delle Comunicazioni
Università di Roma Tor Vergata
Politecnico Milano 1863
KU Leuven
Università di Trento
Gradiant – Galician Research and Development Center in Advanced Telecommunications
Alma Mater Studiorum Università di Bologna
Cefriel – Politecnico di Milano
Sapienza Università di Roma
torino wireless – ICT and Innovation in Piemonte
Boğaziçi Üniversitesi 1863
Consiglio Nazionale delle Ricerche
Università di Napoli UNIPARTHENOPE
Università degli Studi Firenze
The United States Secret Service
Politecnico di Torino
Warwick – The University of Warwick
University of Oxford
AIESEC Alumni Germany
Università degli Studi di Napoli Parthenope
UNINOVA – Instituto de Desenvolvimento de Novas Tecnologias
Università degli Studi di Genova
Link Campus University
cini Cyber Security National Lab
Technische Universität Berlin
European Electronic Crime Task Force

FY23 NUMBERS

Brand Protection

Web monitoring to prevent corporate brand misuse

246 removed

Information Sharing

Information exchange on potential new types of attacks

36.599

IoC Analyzed

VA

VA and PenTest on corporate digital channels

Early Warning

Vulnerability information exchange and "zero day"

29.017

Vulnerabilities detected

mobileCyber Threat Intelligence

Monitor app store to remove unauthorized apps

789

Removed

Big Data Analysis

Correlation and aggregation of heterogeneous data for intelligence purposes

40

Terabyte Analyzed

Cyber Threat Intelligence

Collection and analysis of threats likely to turn into attacks

169.244

Security blocks reported

+28% respect 2022

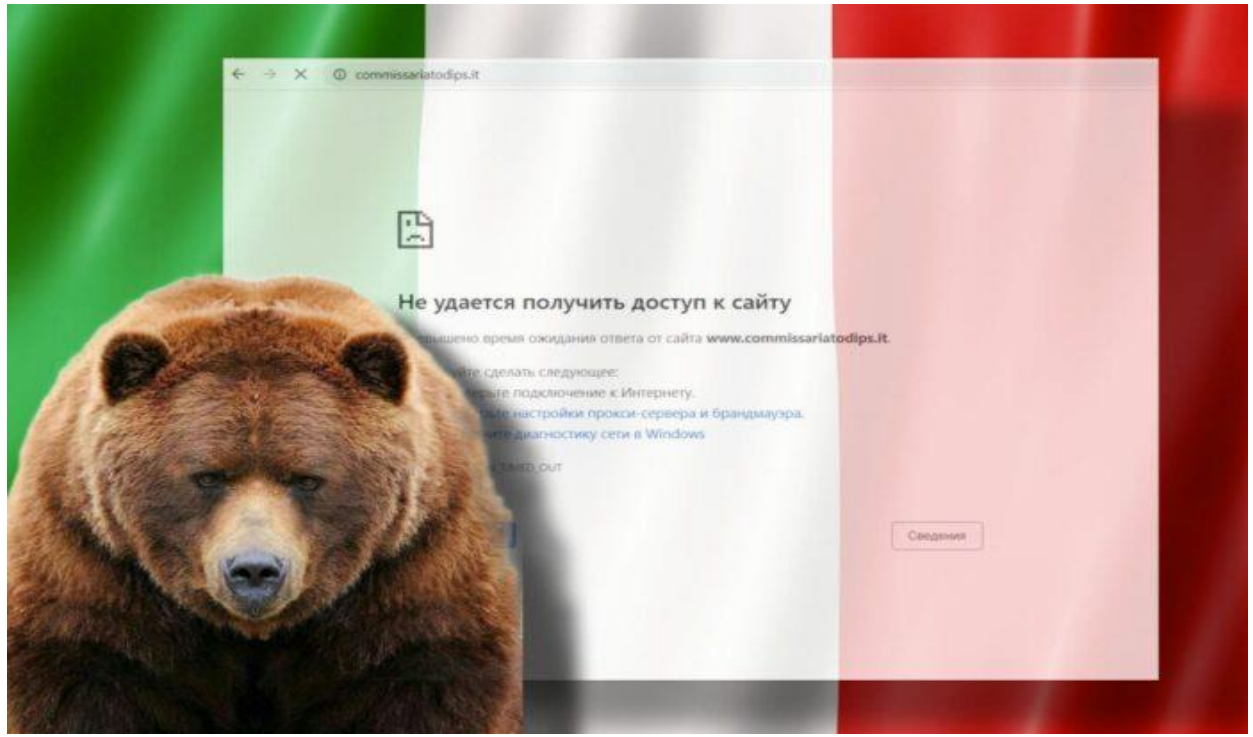
24/7 365 SERVICE

DDOS

During 2023, the emergence of new armed conflicts in the world (particularly the Russian-Ukrainian conflict and in the Middle East) caused new waves of Distributed Denial-of-Service (DDoS) attacks to be generated by emerging pro-Russia hacker groups such as Killnet or NoName057(16).

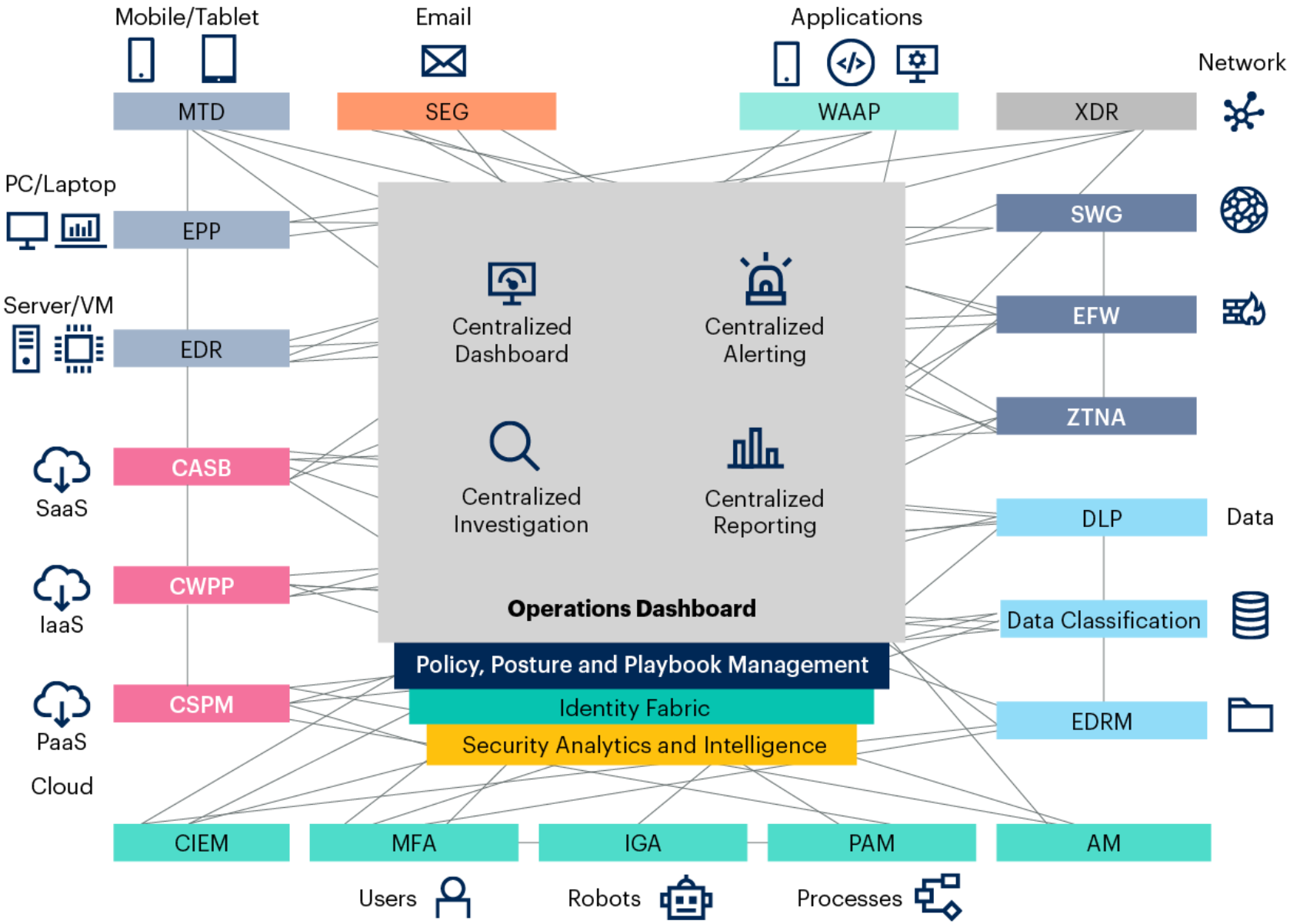
17
attacchi DDOS

438.876
IP bloccati



#Data Driven CERT

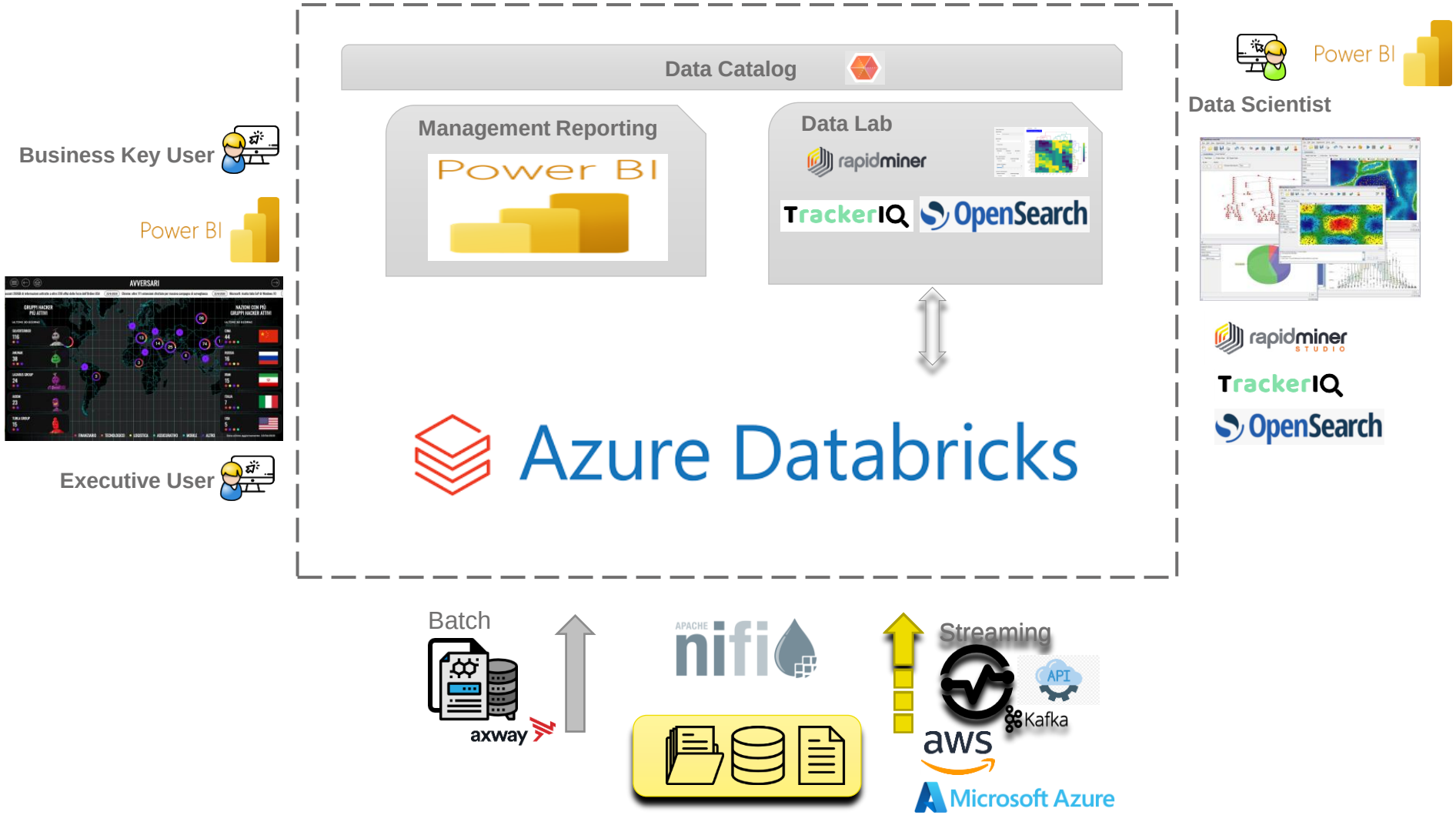
Cybersecurity Mesh Architecture Complete



Source: Gartner
754315_C

Gartner

#DATA LAKEHOUSE



CASE STUDY /EPSS

GOAL

The goal is to prioritize CVEs (Common Vulnerabilities and Exposures) so that those with the highest risk and impact on corporate assets are addressed first, making Cybersecurity defense more efficient.

How to measure risk?

Algorithm
Machine Learning
EPSS

How to measure the impact on business assets?

Algorithm
Magnitudine Host

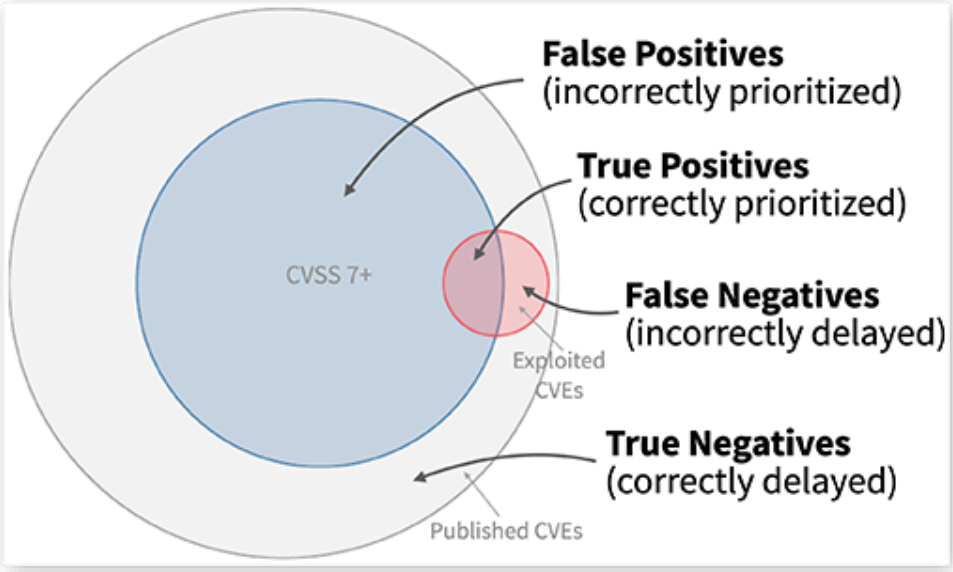
WHY A MACHINE LEARNING ALGORITHM?

Traditional solution

Assign priority to CVEs that have CVSS Score greater than a certain threshold (e.g., CVSS 7+)

Problems:

- Static approach, based on predetermined rules.
- Does not use patterns found in historical data regarding "exploits in the wild"
- Empirically also prioritizes the many CVEs that will not really be exploited in the future (many false positives)



Machine Learning approach

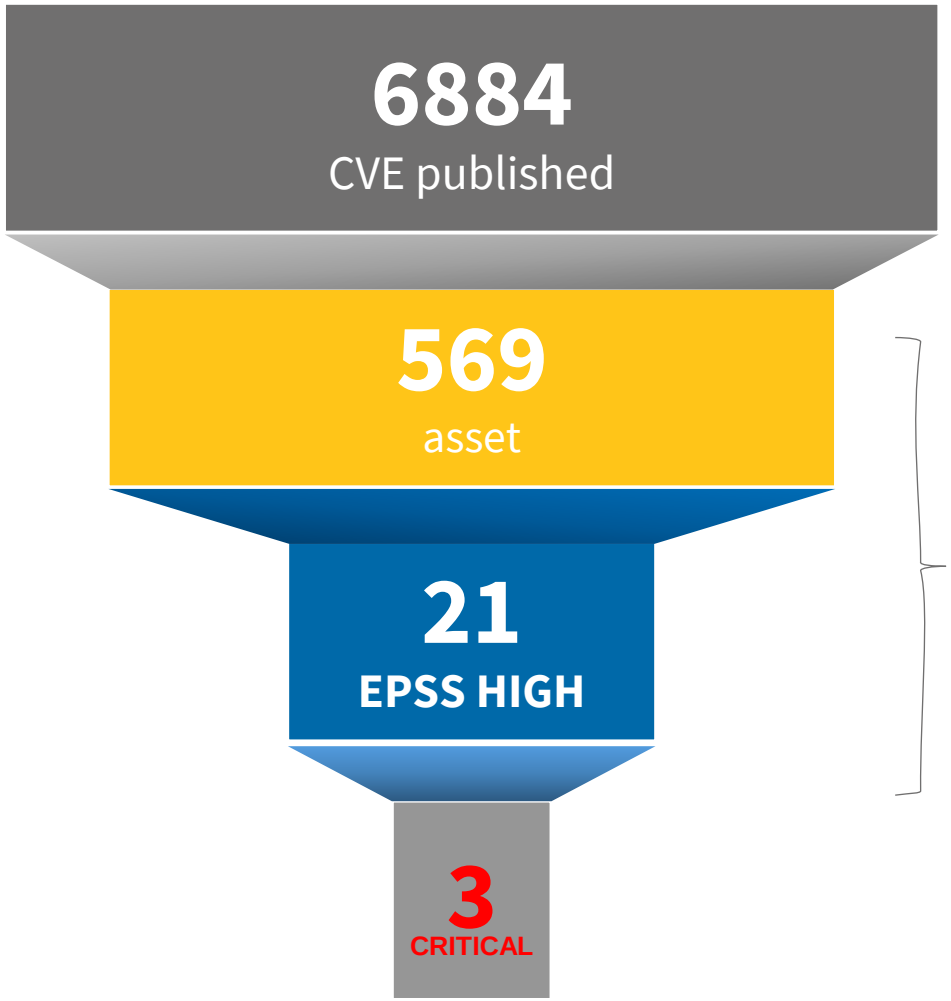
The EPSS is a machine learning algorithm that predicts the probability of a CVE being exploited in the wild.

SOURCE

Source	Description	Data
NVD (National Vulnerability Database)	Vulnerabilità di sicurezza informatica divulgate pubblicamente (CVE) e score e attributi forniti dal Common Vulnerability Scoring System (CVSS)	CVE, CVSS Score e Attributi
Exploit DB	Informazioni sui codici pubblicati per lo sfruttamento della vulnerabilità	Esistenza di codici pubblicati per lo sfruttamento
Fortiguard	Informazioni sulle vulnerabilità realmente sfruttate con successo	Esistenza di codici sfruttati “in the wild”
AlienVault		
Cisa Catalog		
FIRST.ORG	EPSS V2 score basato dal modello accademico FIRST.ORG	EPSS V2 score
Fortiguard Threat Signal	Informazioni sulle vulnerabilità realmente sfruttate con successo	Esistenza di codici sfruttati “in the wild”
TS-WAY Intelligence		

RESULTS

February 2023



-92%

-97%

Relevance:
Reduced effort through an algorithm
Host Magnitude

Efficiency:
Effort reduction by algorithm
EPSS

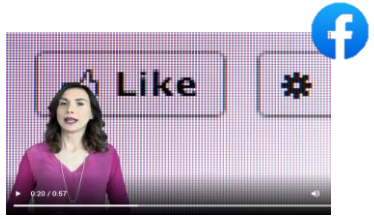
MORE…


#Behaviour Control


N L P

HUMAN FACTOR…

SOCIAL MEDIA



MOBILE E APP

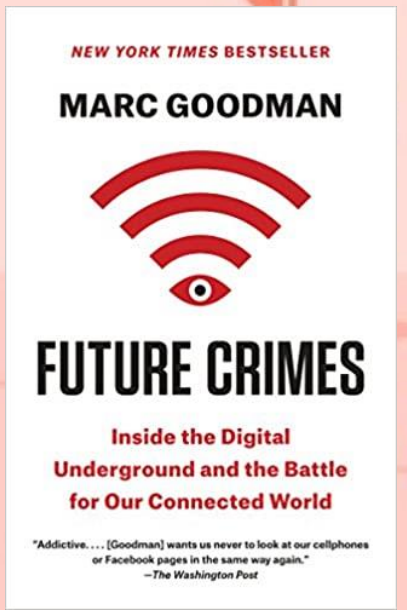
FAKE NEWS

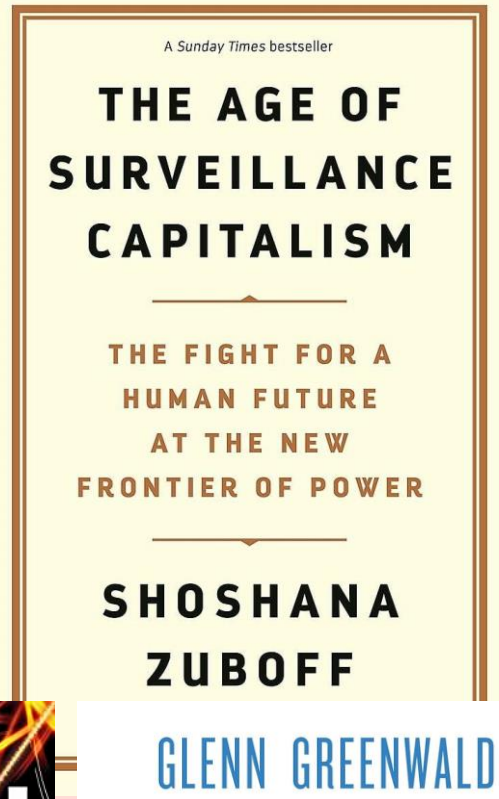
MALWARE E RANSOMWARE

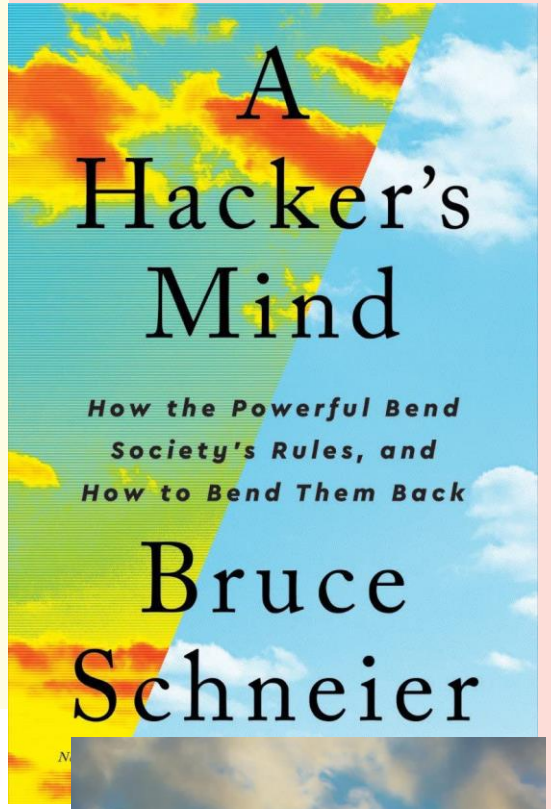
Posteitaliane

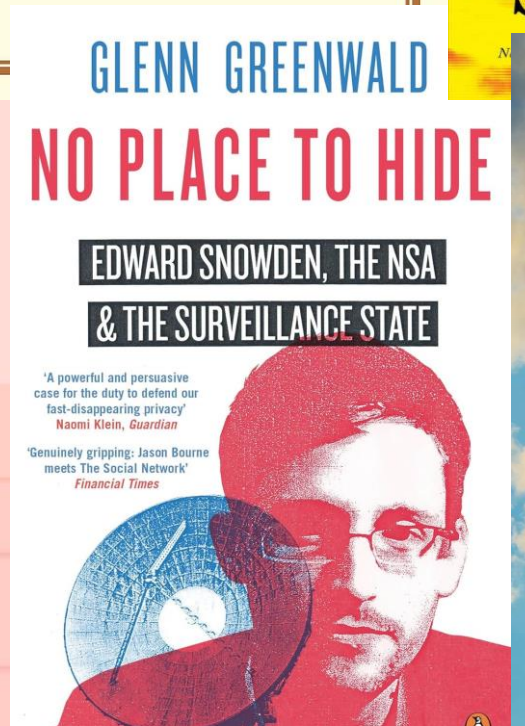
CERT Posteitaliane

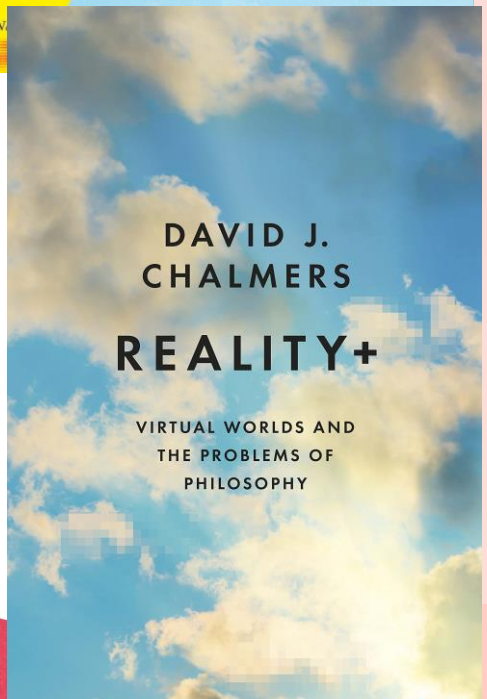
#ioleggocyber












cert@posteitaliane.it