Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Un approccio sinergico tra cybersecurity e protezione dei dati personali

Stefano Moni, Direttore Ufficio Protezione Dati, Direzione Centrale della Polizia Criminale

Alessandro Vallega, Chairman, Clusit Community for Security

21 marzo 2024, h. 14.00

Agenda

01 Italian law enforcement organization

in varietate concordia

02 Data protection @ the Central Directorate of Criminal Police

A peculiar case

03 Innovation

From the European Directive to a daily practice

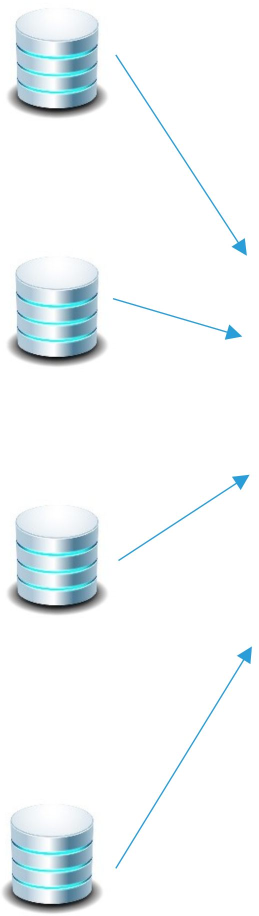
Italian Police Forces and data protection

Polizia di Stato
(DPO)

Arma dei Carabinieri
(DPO)

Guardia di Finanza
(DPO)

Polizia Penitenziaria
(DPO)



Central Directorate of Criminal Police

Inter-agency Joint Information Systems

National Criminal Database (SDI)	National DNA Database	Schengen Information System	Passenger Name Records	112 Emergency telephone number	IT- NCB

DPO

(me!)

Inter-agency joint information systems

some figures

National criminal database

> 1 billion records (subjects, objects, facts)

> 162k users

> 40k workstations (fixed + mobile)

> 12k DSAR per year

National Schengen Information System

> 600 Mln queries per year

> 8k DSAR per year

> 1 Mln queries on fingerprints

National DNA database (born in 2017)

> 300k samples taken from subjects (still in the process of recording)

> 100k records in the system (from samples + crime scenes)

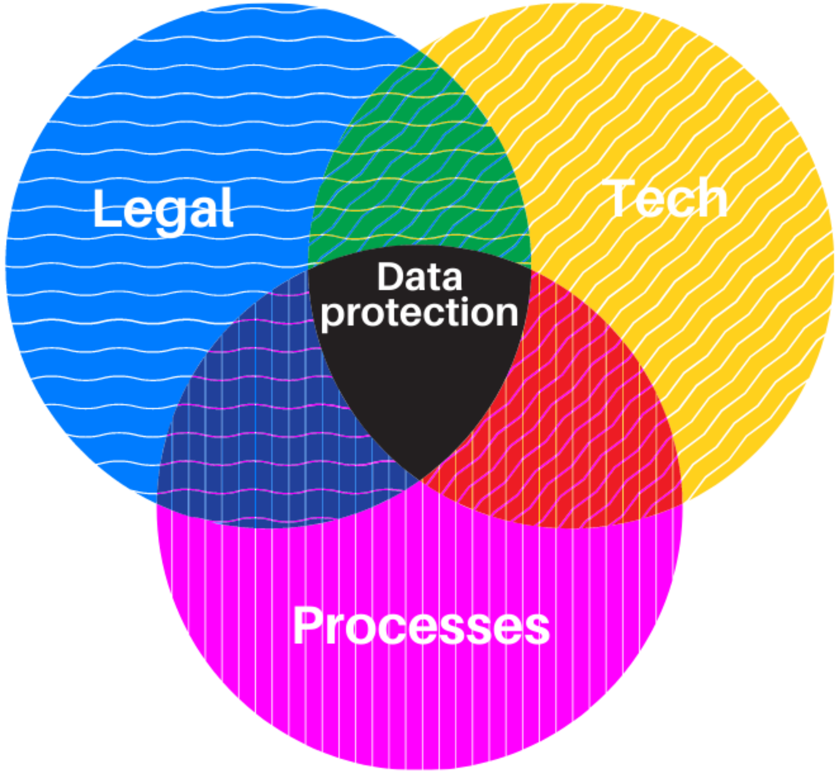
Data Protection Office tasks @ Central Directorate of Criminal Police

more than a DPO

- Point of contact Garante privacy
- International WGs (CPD, EDEN, COM)
- Chair Data Breach government WG
- National cybersec policy WG
- Cyber Security Operations Center
- Vulnerability assessments (apps + sys)
- Education program > 3.000 ppl (all ranks)
- Audits
- Risk analisys (in-house *ad hoc* software)
- Directives and guidance on security plans

Data Protection Office skills

not an easy task



The protection of personal data is an inherently interdisciplinary matter

this IS a strategic factor

The approach: processes are key
an example

2018

Attuazione del D. Lgs. 53 del 2018
Assessment sulla protezione dei dati

Azioni, ruoli e responsabilità

DIREZIONE CENTRALE DELLA POLIZIA CRIMINALE
Ufficio per la Sicurezza dei Dati

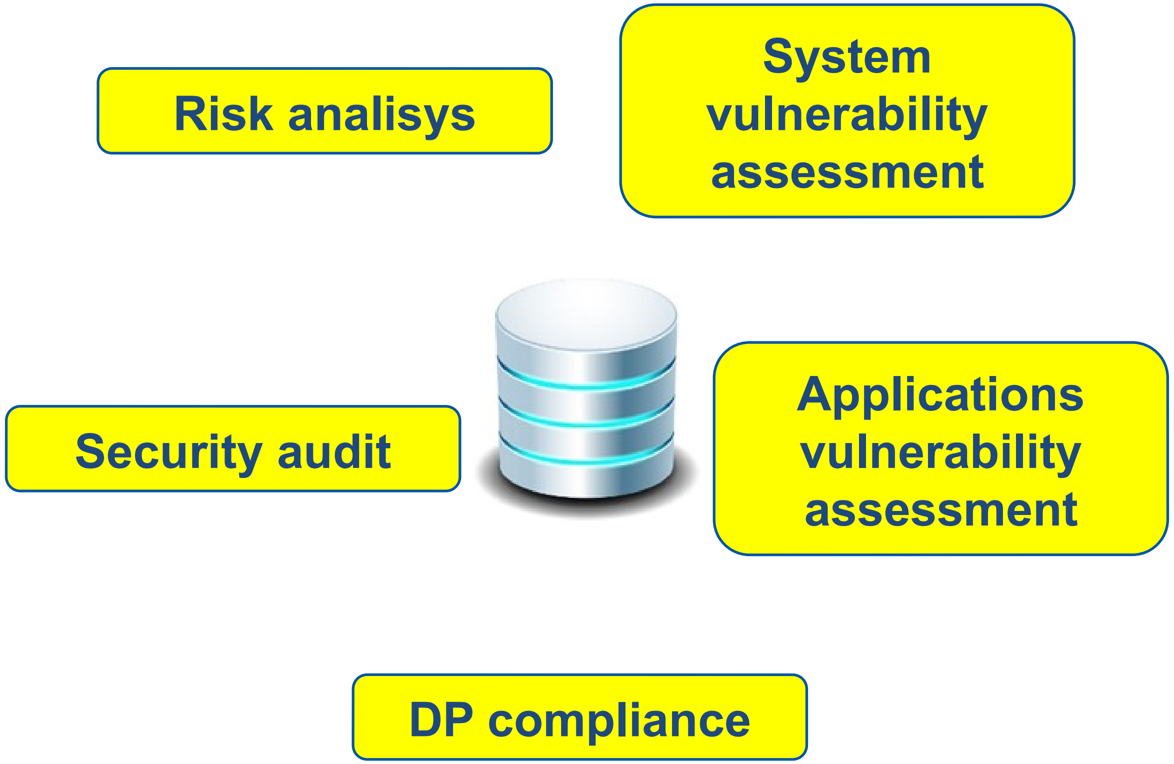
PER USO ESCLUSIVO DI UFFICIO

Assessment over DP needed to implement PNR Directive

- from law provisions to effective actions
- definition of processes and procedures
- technical and organizational requirements
- roles and responsabilities (RACI matrix)
- data protection agreement with processor
- system requirements by the DPO

data protection by design and by default

The approach: a holistic cycle



Risk analisys

System vulnerability assessment

Security audit

Applications vulnerability assessment

DP compliance

PROs

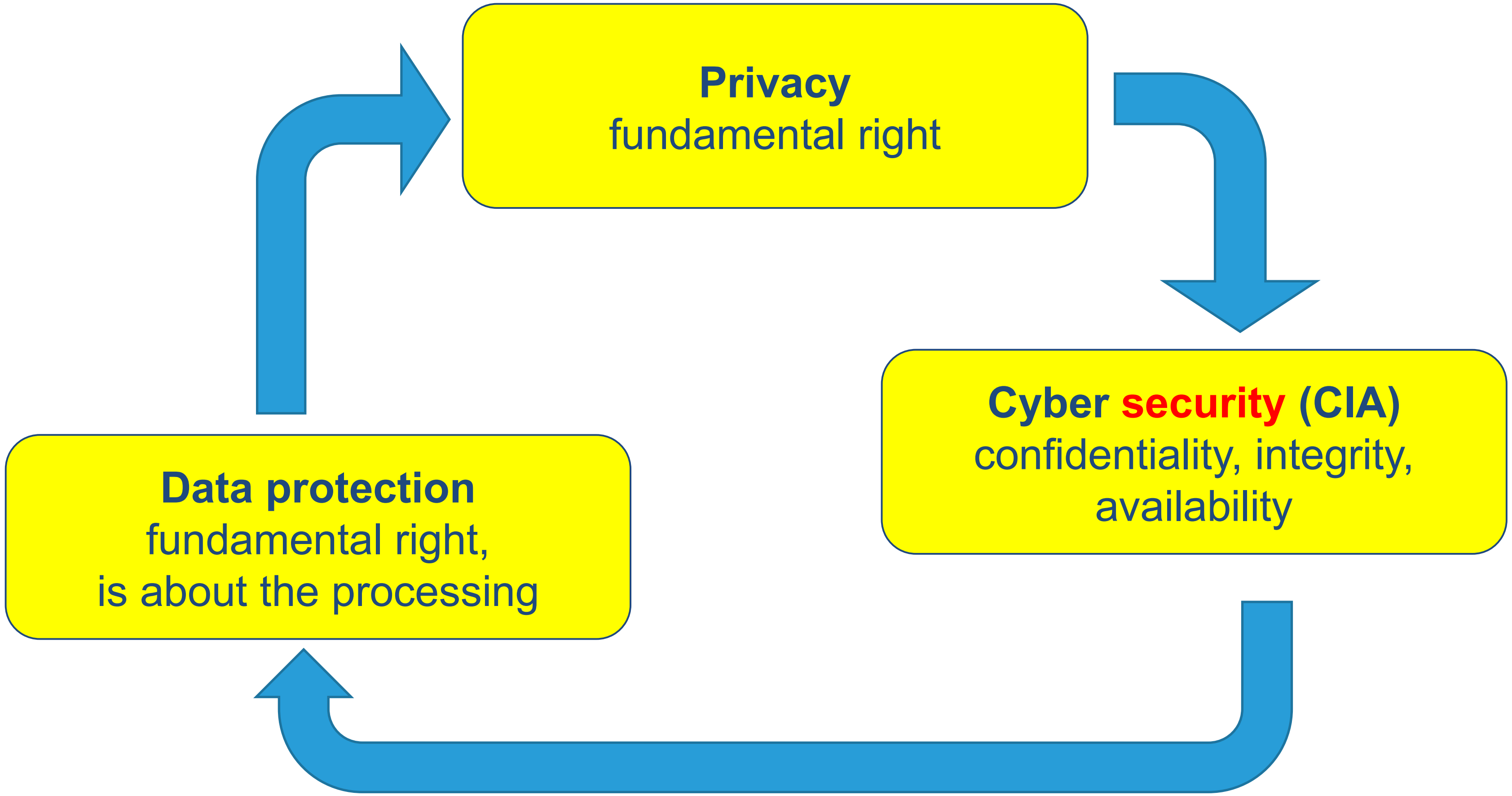
- Cross checked results mean coherent and consistent results
- Enhanced awareness both at executive and operational level
- International standards (inspired, **not** certified!)
  - ✓ ISO/IEC 27001:2013
  - ✓ ISO 9001:2008

CONs

- Effort
- Time consuming

Data Protection and cybersecurity

close relatives



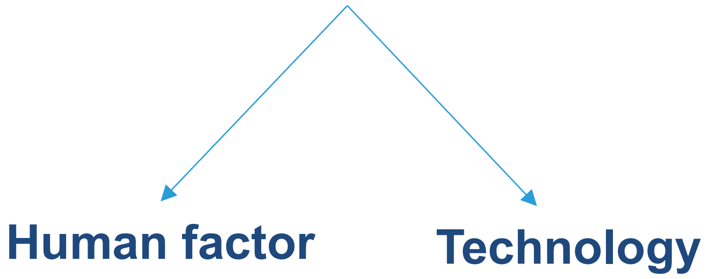
Privacy
fundamental right

Cyber security (CIA)
confidentiality, integrity, availability

Data protection
fundamental right,
is about the processing

LED definition of a data breach
(recital #11)

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data"



Human factor

Technology

Data Protection and cybersecurity

close relatives

LED Requirement (Art. 30):

…notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority…

A “simple” question:

How can I notify the supervisory authority about a ***data breach*** *if I am not even aware I am having one?*

Two aspects:

Human factor and technological

Data Protection and cybersecurity

a holistic approach: the Cyber Security Operations Center (started ops April 2021)

- **Vision:**
  - ✓ Convergence of information security functions with data protection
  - ✓ First mosaic tile of the national strategic cyber perimeter
  - ✓ First of its kind in the Police Forces

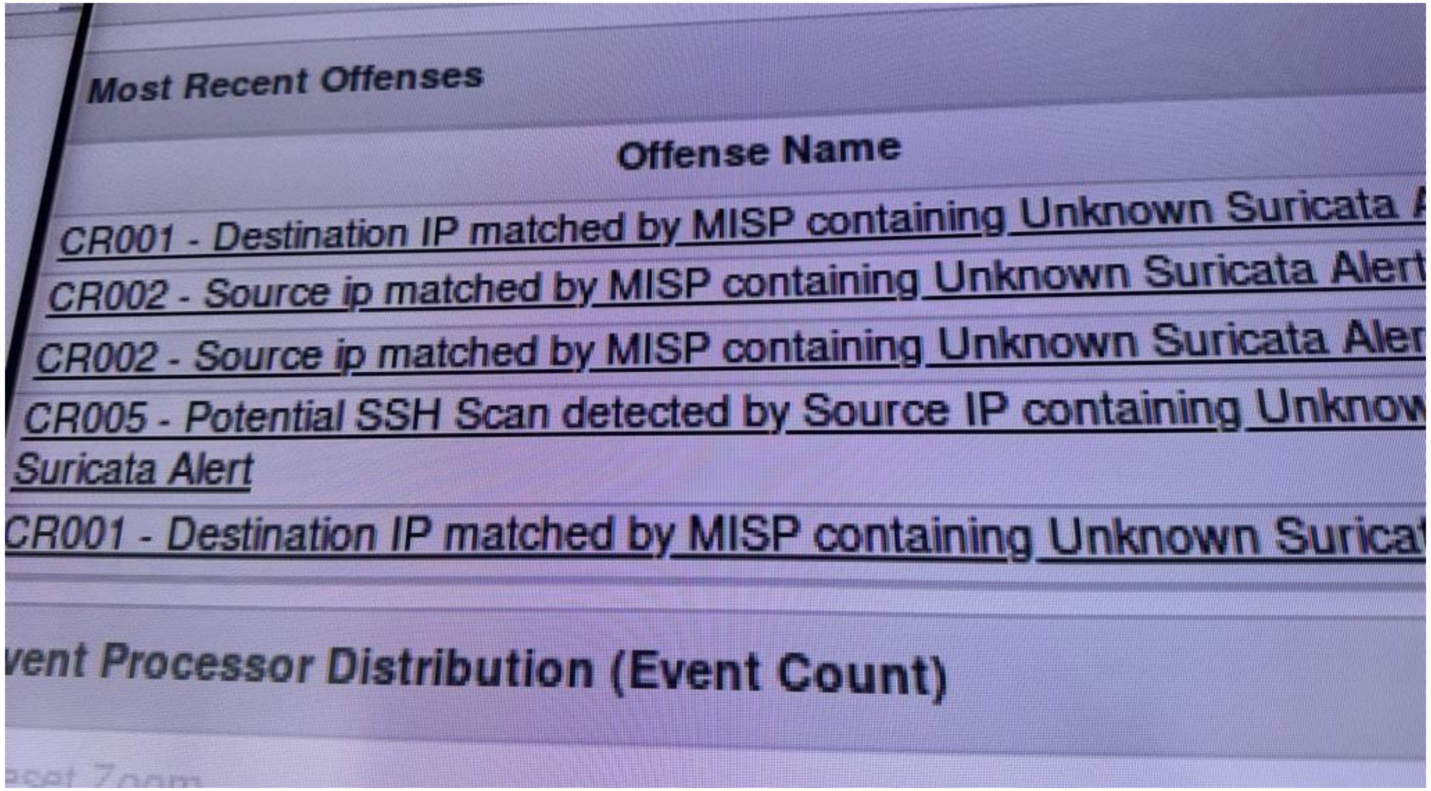
- **Main features:**
  - ✓ Definition of new processes compliant with ISO standards for incident monitoring and management
  - ✓ Different dashboards and tools for DP and CS
  - ✓ SIEM: up to 7.500 events per sec (average 1.200)

Data Protection *and* cybersecurity

25-29 May 2023 exercise: a simulated massive cyber campaign to the infrastructure

- **Actors:**
  - ✓ Central Directorate of Criminal Police (C-Soc)
  - ✓ Postal and Communication Service (CERT)
  - ✓ Private party (Attack Team, ad-hoc platform)

- **Main types of attack**
  - ✓ Brute force
  - ✓ Ransomware from infected email
  - ✓ Credential theft from infected email
  - ✓ DB exfiltration
  - ✓ Command and control privilege escalation
  - ✓ XSS to the web access portal
  - ✓ …



Most Recent Offenses

Offense Name

CR001 - Destination IP matched by MISP containing Unknown Suricata A

CR002 - Source ip matched by MISP containing Unknown Suricata Alert

CR002 - Source ip matched by MISP containing Unknown Suricata Aler

CR005 - Potential SSH Scan detected by Source IP containing Unknow
Suricata Alert

CR001 - Destination IP matched by MISP containing Unknown Surica

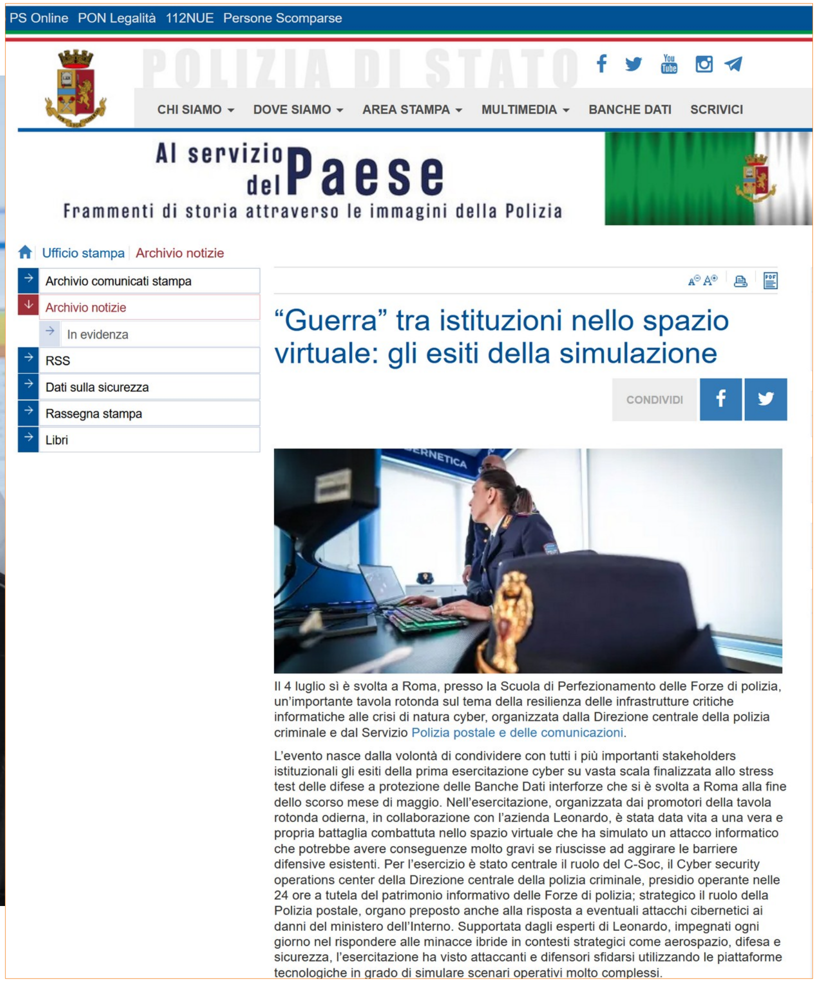
vent Processor Distribution (Event Count)

eset Zoom

Data Protection and cybersecurity

25-29 May 2023 exercise: a simulated massive cyber attack to the infrastructure

- 3 sites
- 55 attacks
- 27 attacks report
- 5 operations days
- 48 professionals
- 3 organizations
- 5 months of preparation



"Guerra" tra istituzioni nello spazio virtuale: gli esiti della simulazione

Il 4 luglio sì è svolta a Roma, presso la Scuola di Perfezionamento delle Forze di polizia, un'importante tavola rotonda sul tema della resilienza delle infrastrutture critiche informatiche alle crisi di natura cyber, organizzata dalla Direzione centrale della polizia criminale e dal Servizio Polizia postale e delle comunicazioni.

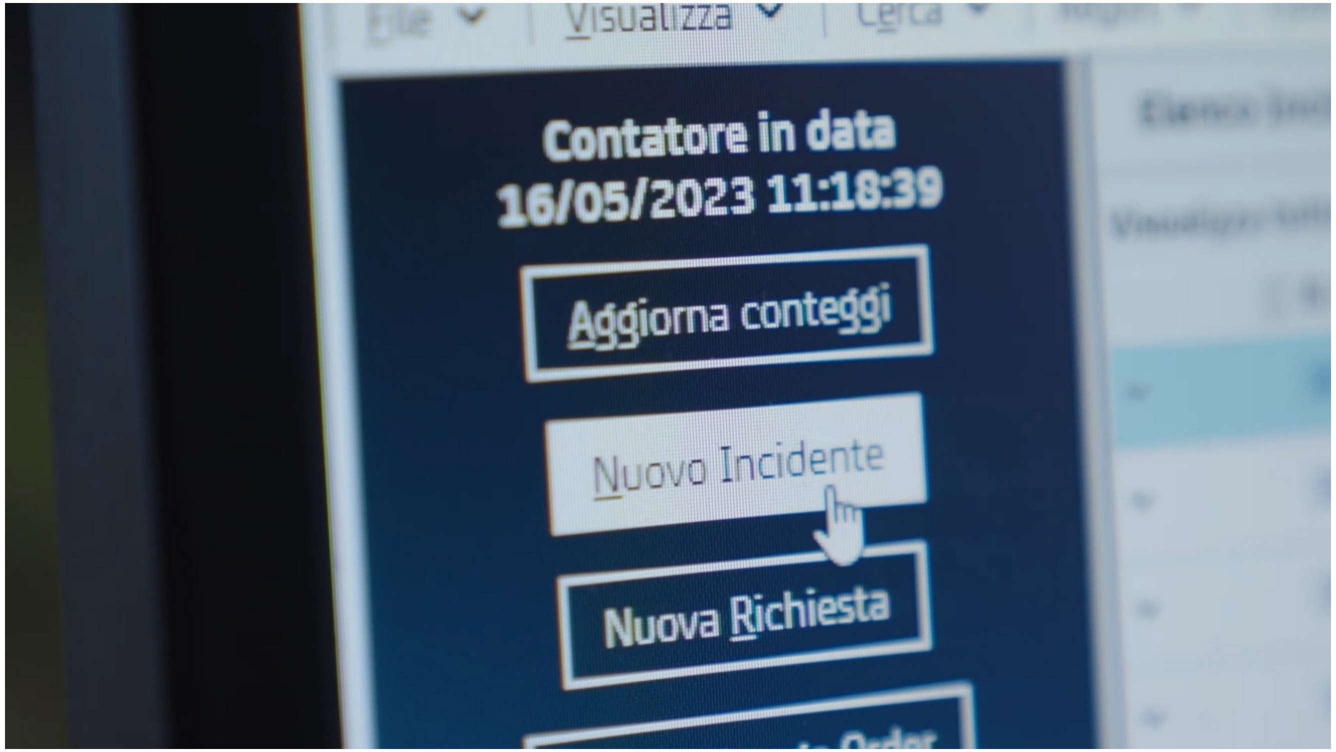
L'evento nasce dalla volontà di condividere con tutti i più importanti stakeholders istituzionali gli esiti della prima esercitazione cyber su vasta scala finalizzata allo stress test delle difese a protezione delle Banche Dati interforze che si è svolta a Roma alla fine dello scorso mese di maggio. Nell'esercitazione, organizzata dai promotori della tavola rotonda odierna, in collaborazione con l'azienda Leonardo, è stata data vita a una vera e propria battaglia combattuta nello spazio virtuale che ha simulato un attacco informatico che potrebbe avere conseguenze molto gravi se riuscisse ad aggirare le barriere difensive esistenti. Per l'esercizio è stato centrale il ruolo del C-Soc, il Cyber security operations center della Direzione centrale della polizia criminale, presidio operante nelle 24 ore a tutela del patrimonio informativo delle Forze di polizia; strategico il ruolo della Polizia postale, organo preposto anche alla risposta a eventuali attacchi cibernetici ai danni del ministero dell'Interno. Supportata dagli esperti di Leonardo, impegnati ogni giorno nel rispondere alle minacce ibride in contesti strategici come aerospazio, difesa e sicurezza, l'esercitazione ha visto attaccanti e difensori sfidarsi utilizzando le piattaforme tecnologiche in grado di simulare scenari operativi molto complessi.

Data Protection and cybersecurity

25-29 May exercise: a simulated massive cyber attack to the infrastructure

Lessons learned

- ✓ Human factor carries a much higher **risk** than the technological one
- ✓ **Panic** is difficult to avoid: have clear and easy procedures in place
- ✓ **Technology is not enough**, you've got to stress-test the system (and the people)
- ✓ Timing is key: **threat intelligence** doesn't work if you do not promptly *onboard* IoCs
- ✓ **Resilience** CAN be raised



MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

Thanks for your attention

Q&A

DIREZIONE CENTRALE DELLA POLIZIA CRIMINALE
UFFICIO PROTEZIONE DATI