Experiences from an operational SOC/CERT

Cybersecurity Webinar: CERT and SOC for Air Navigation Services

> Foreword

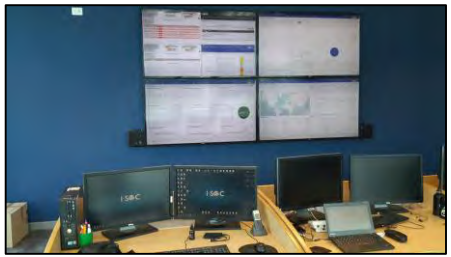
*Our goal is to ensure the **safety** and punctuality of the **millions of passengers** who fly in Italian airspace, while contributing to the growth of national and European air transport through ongoing efficiency and innovation.*

«Duty of Care»

enav group

> Security Mission in ENAV

"Protecting people, infrastructures, technology and systems from unlawful interference, even if not deliberated, which may interfere with information availability, integrity and confidentiality"



Grant security of

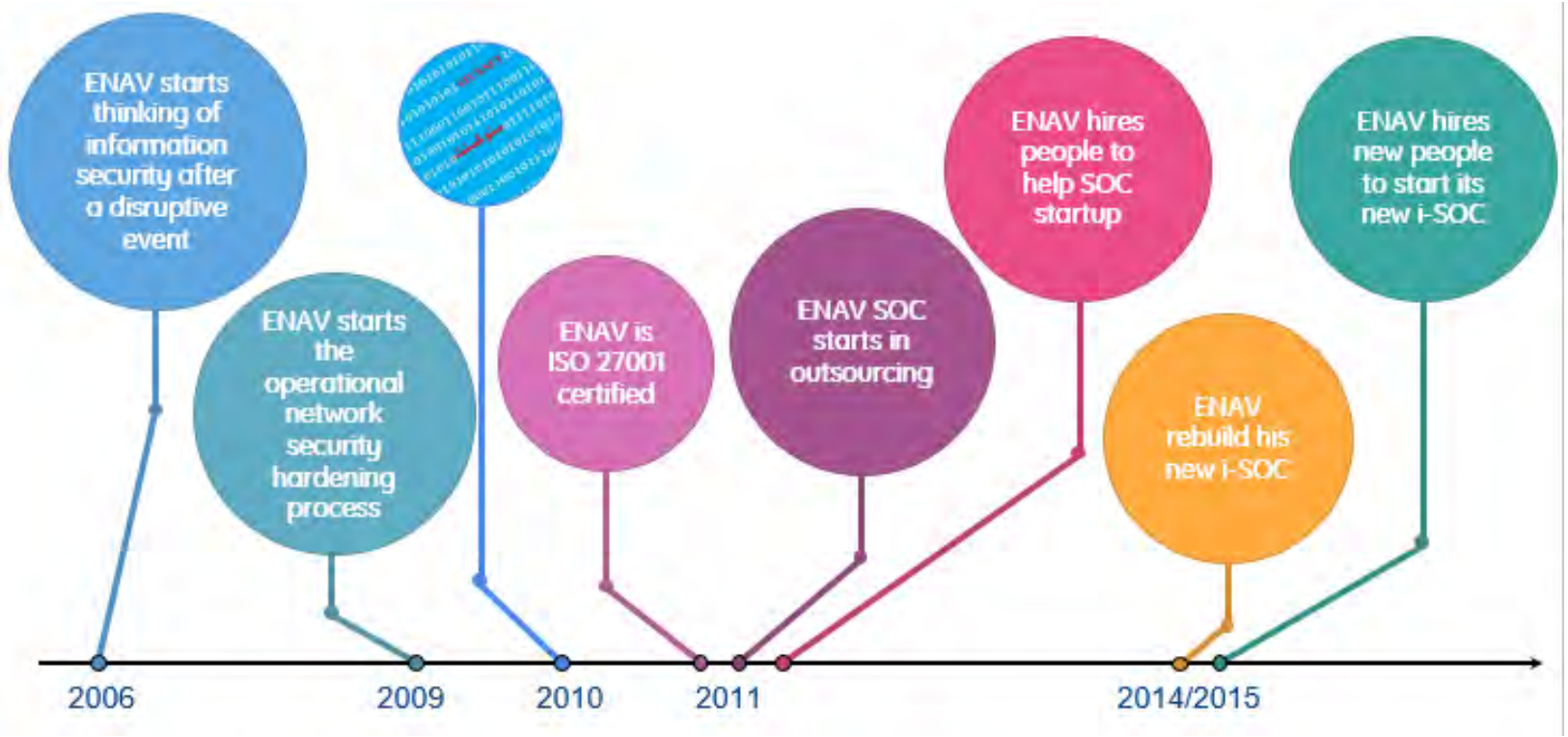
- people
- physical infrastructures
- information, systems and network

> Constraints

- Complex, multilayered environment;
- The empire of legacy systems;
- Need to collect events and logs from lot of different systems and use a common model;
- On top of the model apply all SecMS controls in the same way
- challenging regulatory framework

TEMPUS FUGIT

> Lesson learned

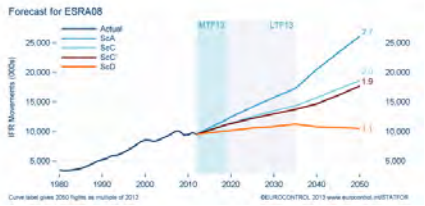


Rebuild learning from the past errors

Redesign from scratch


QUALITY


TRAFFIC


Forecast for ESRA08
Actual
ScA
ScB
ScC
ScD
IFR Movements (000s)
25,000
20,000
15,000
10,000
5,000
1980
1990
2000
2010
2020
2030
2040
2050
MTF13
LTF13
7.7
2.0
1.9
1.1

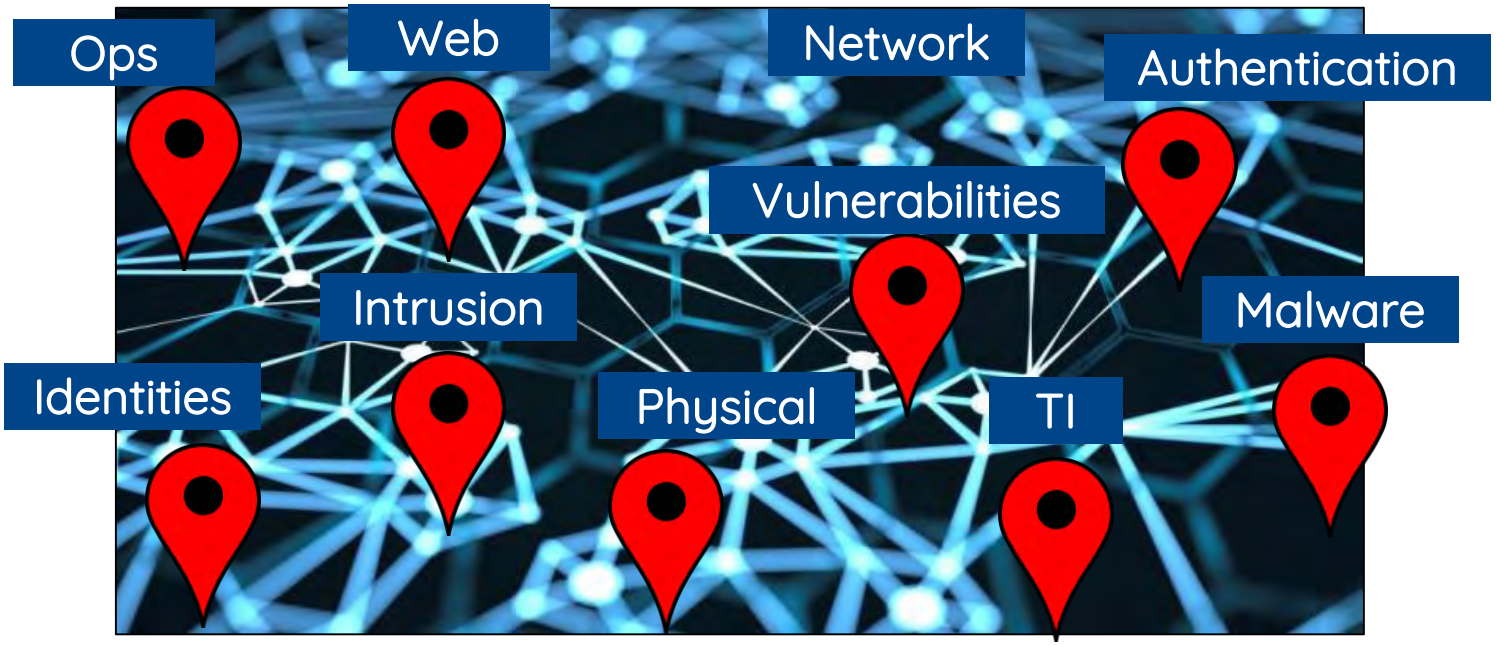

SPEED


EFFICIENCY


MIN
COSTS

enav group

> Needs

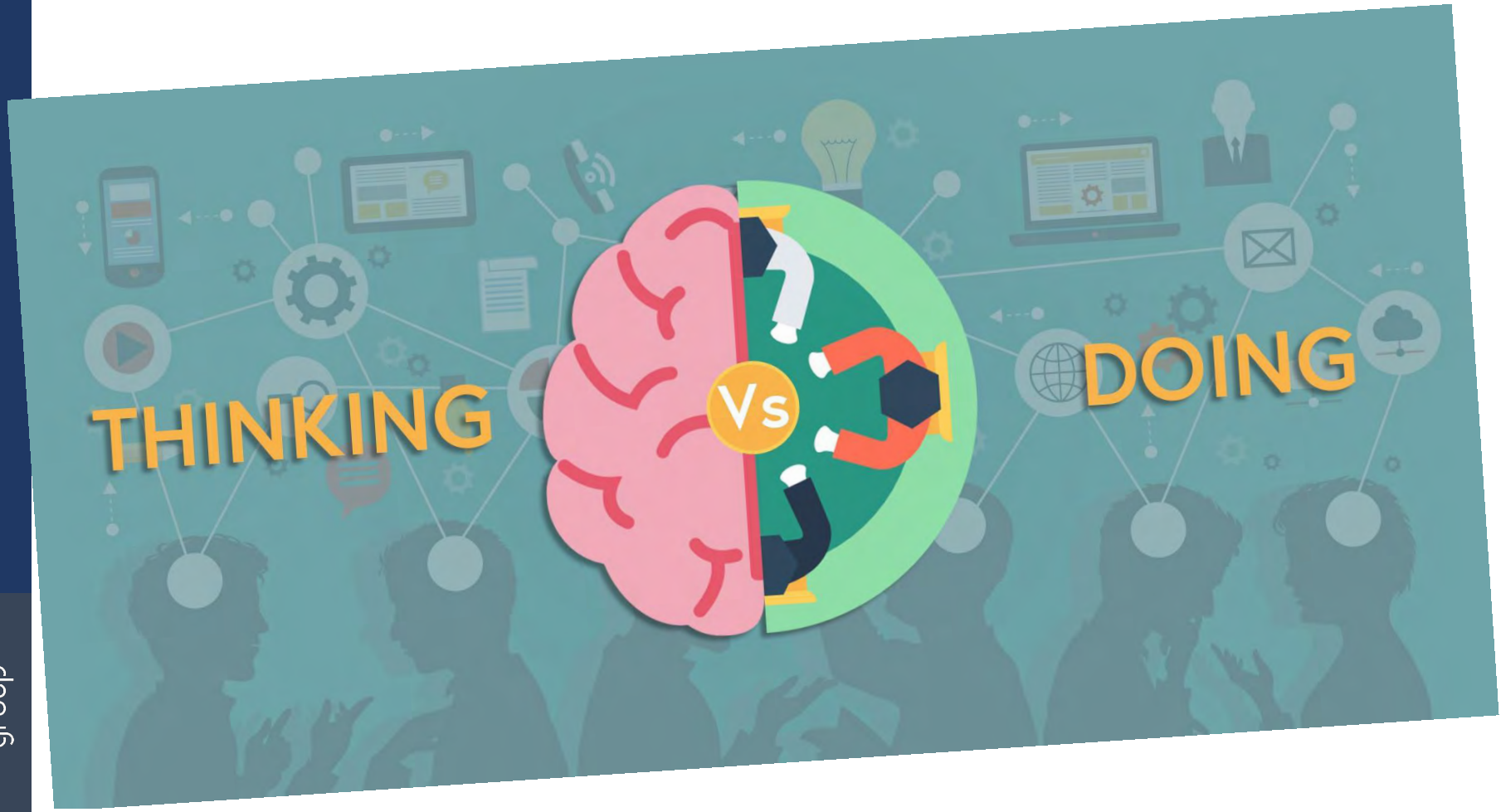


Identify security domains and monitoring zones with the objective of understanding data that will be used only for security purposes

> Critical issues

- Coordination with other ENAV (groupwide) departments
- Data import with no impacts on ops
  - syslog, agents etc
- Background noise deleted
- Exactly understand what we are importing to “send” the data to the right security domain

Here is essential the commitment derived from governance process


THINKING
Vs
DOING

> Tailoring

We built a custom application “on top” of big data crowler adapted for harmonize different set of data

- Built on ENAV needs;
- Focus on ATM ops environment;
- High level of automation;
- Continuous improvement;
- Low operational costs
- Open Source!

- Daily updated to follow new threats
- Reduce false positive;
- Considering human behaviors;
- Automation → Speed!!
- Ready for virtual and cloud

> Services

I-SOC

Security

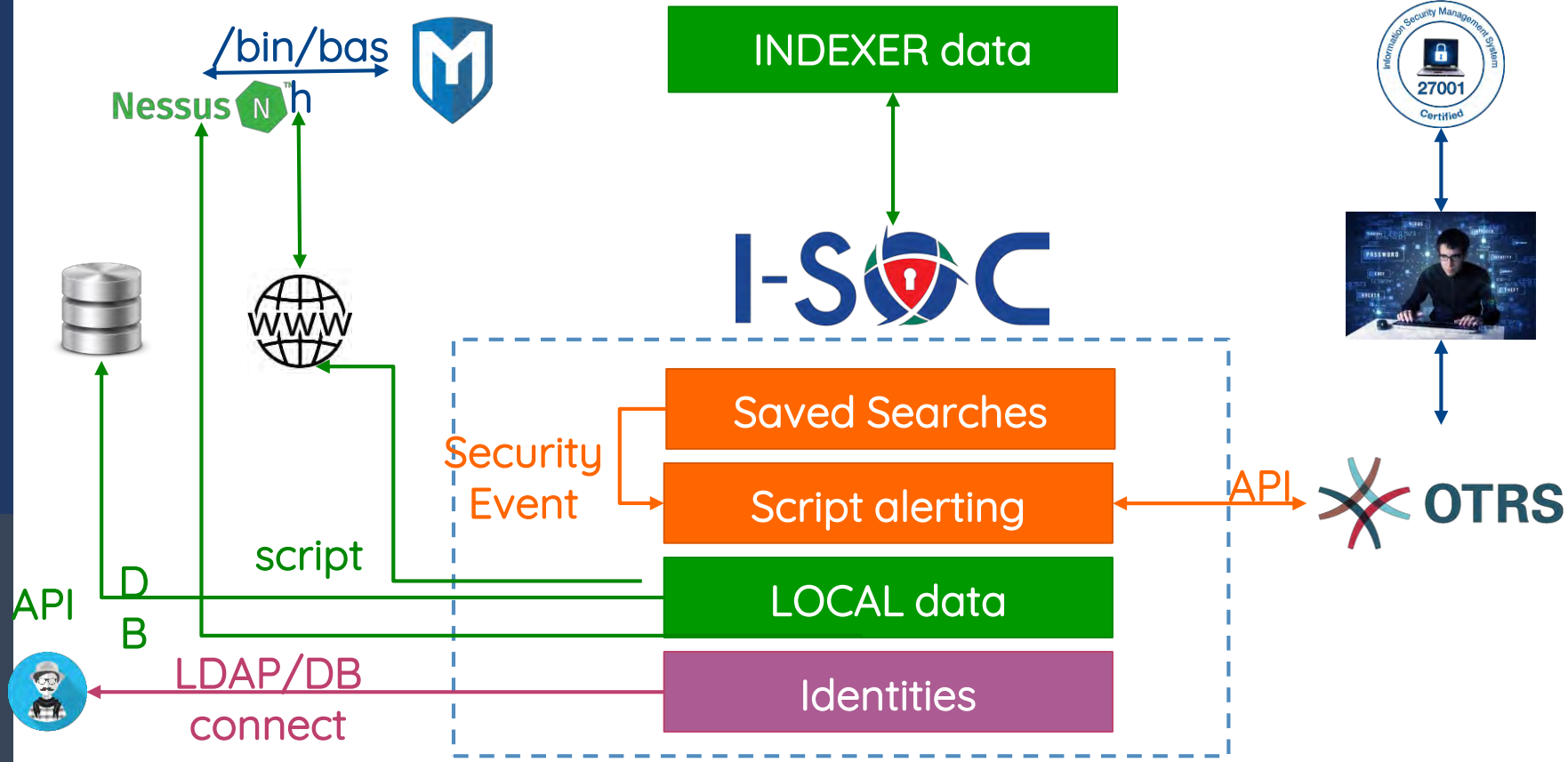
Governance

Information Security Operation Center

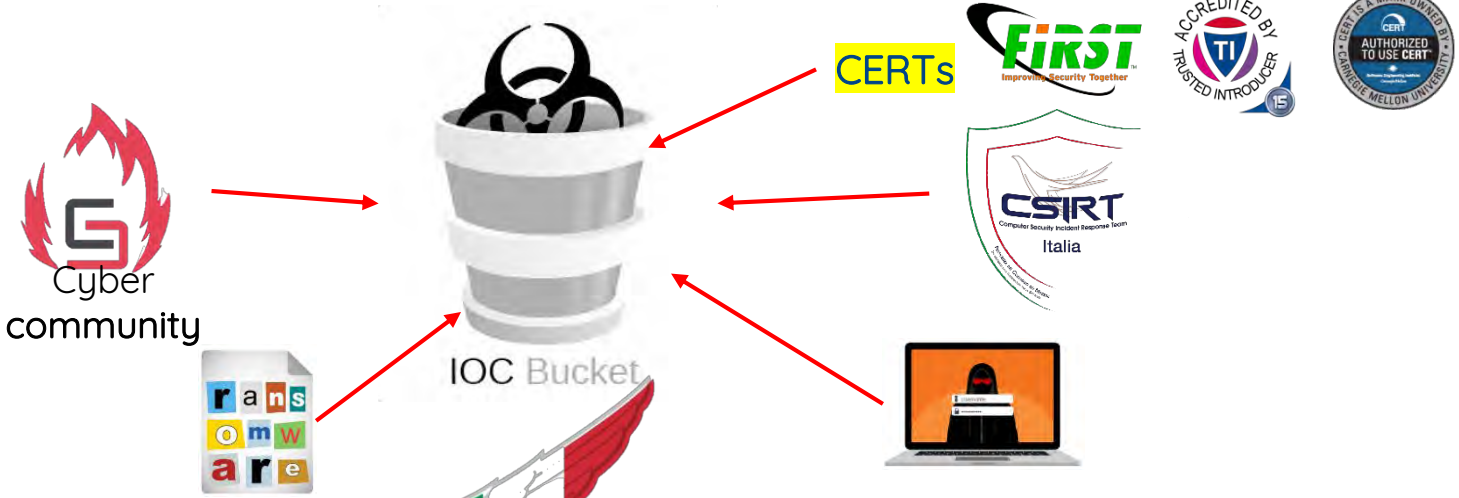
- Security Event Monitoring
- Authentication Authorization Accounting
- Endpoint Protection
- Security Intelligence
- Incident Handling & Response
- Policy Enforcement
- Policy Compliance
- Pen Test / Vuln Assessment
- Forensic
- Security Awareness Attack Simulation
- Lesson Learned & Dissemination
- IT Operation
- Asset & Identity Management

enav group

> make integration



> Threat Intelligence



STIX TAXII

IT-AVIATION ISAC

[IPs, URLs]

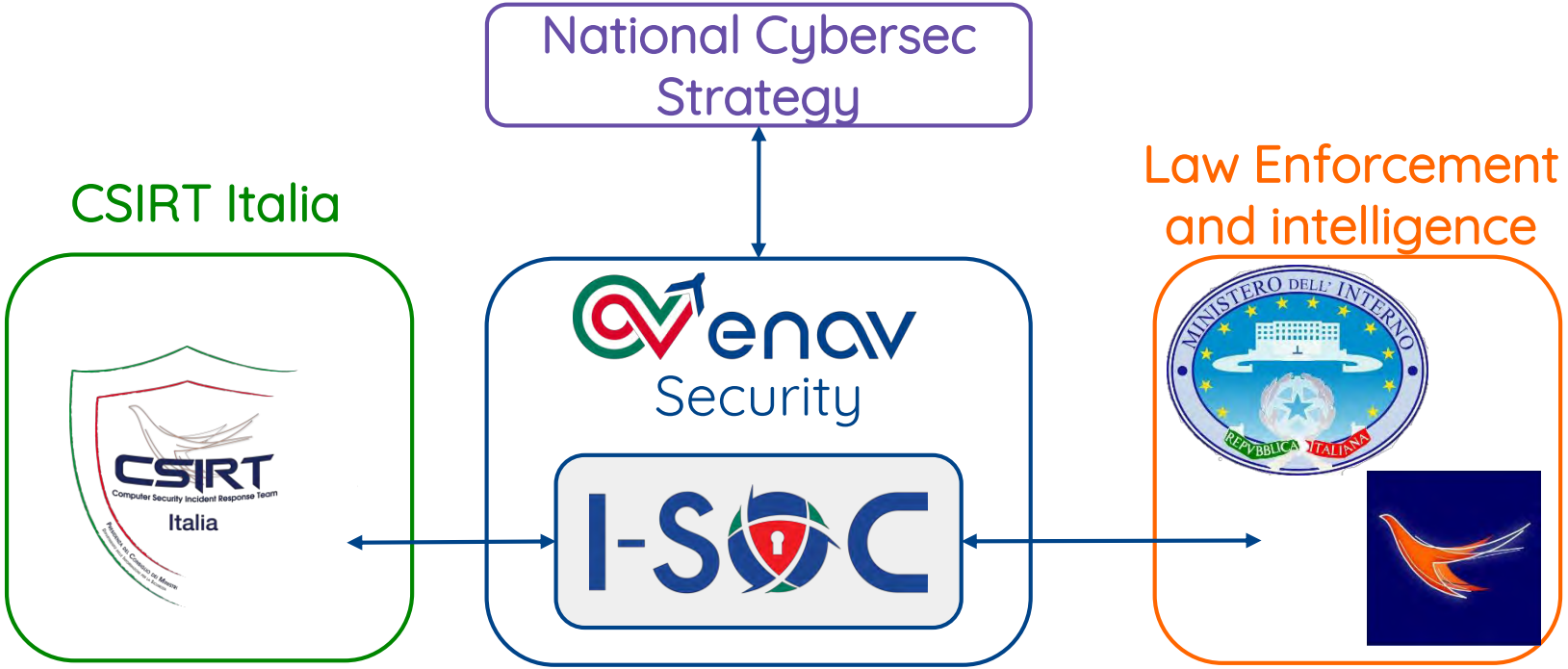
soc_web_ioc_monitorig.csv

Right-click the table cells for more editing options

1	field	dest
216	URL	admin.adoma-jawel-manufact.com/cgi-bin2/kc21.exe
217	URL	all400pples.org.in/molina/fre.php
218	dominio	antiquesonbroad.com
219	URL	antiquesonbroad.com/wp-includes/customize/newchn/index.php
220	dominio	arihanttradersngp.com

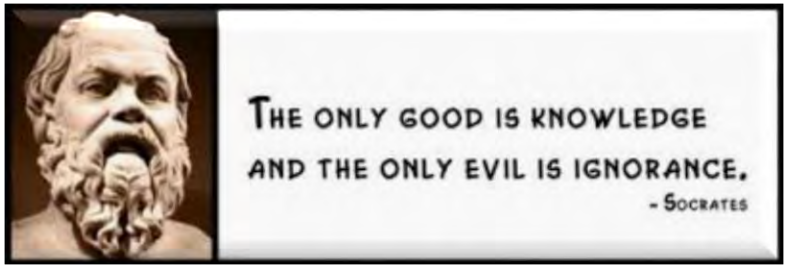
https://scubarda.com/2018/03/31/minemeld-threat-intelligence-automation-connect-to-an-taxii-service/

Designed for fitting the italian cyber security integrated system (NIS Directive and Italian National Cybersec perimeter)



> Takeaways

- UNDERSTAND WHO ARE YOU
- ONE SIZE DOESN'T FIT ALL
- IDENTIFY YOUR NEEDS
- BE A VERY DEMANDING CLIENT
- IDENTIFY YOUR VULNERABILITIES
- HUMAN FACTOR!
- REDUCE THE ATTACK SURFACE
- AVOID COMPLACENCY
- CHALLENGE YOUR ORGANIZATION



- NEVER GIVE ANYTHING FOR GRANTED

Thank You!